ZOOM
TECHNOLOGIES

CCNA | Cisco Certified Network Associate

Course Presentation

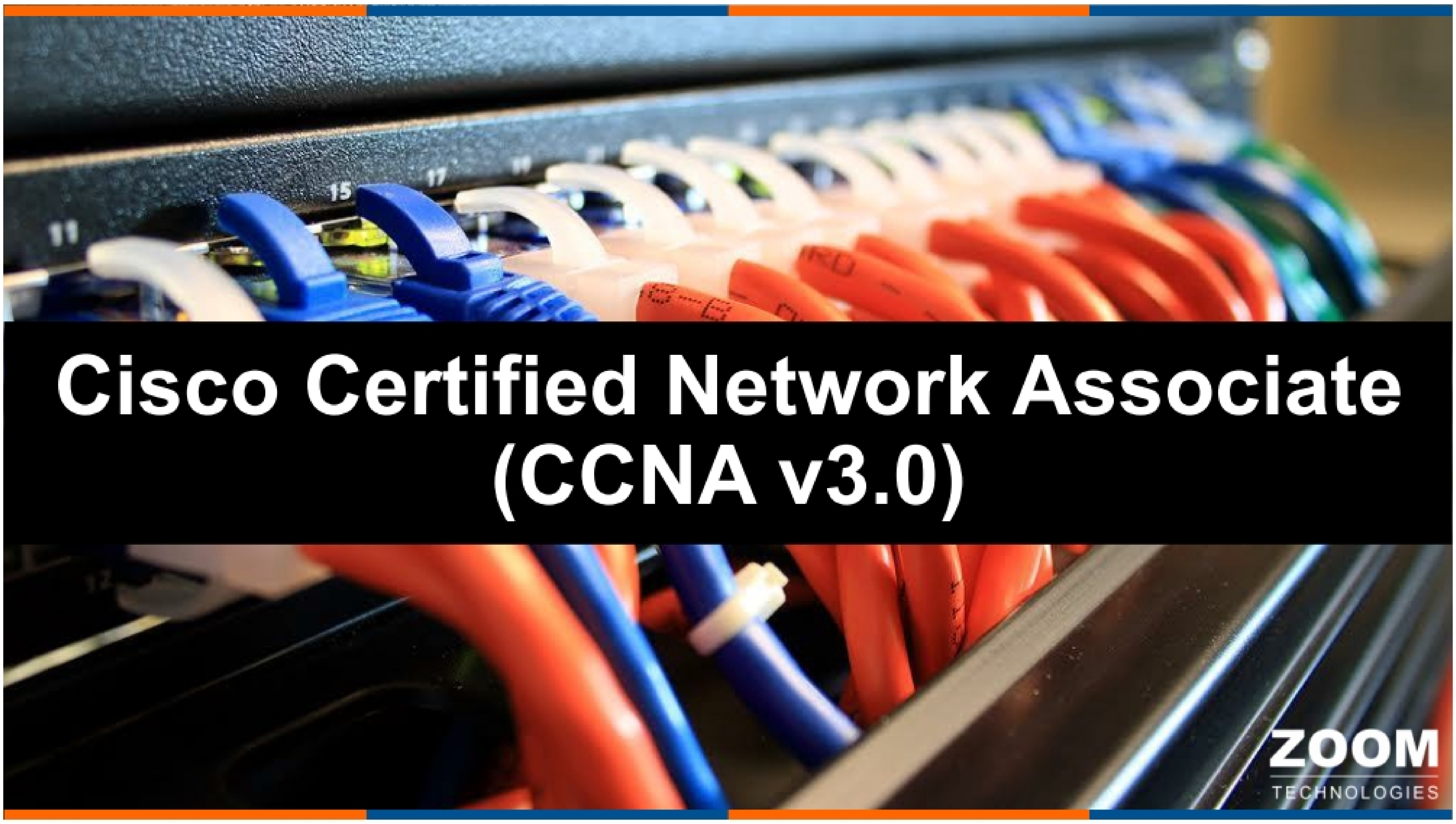
CCNA

(Cisco Certified Network Associate)

Certification Mapped Course

Routing and Switching

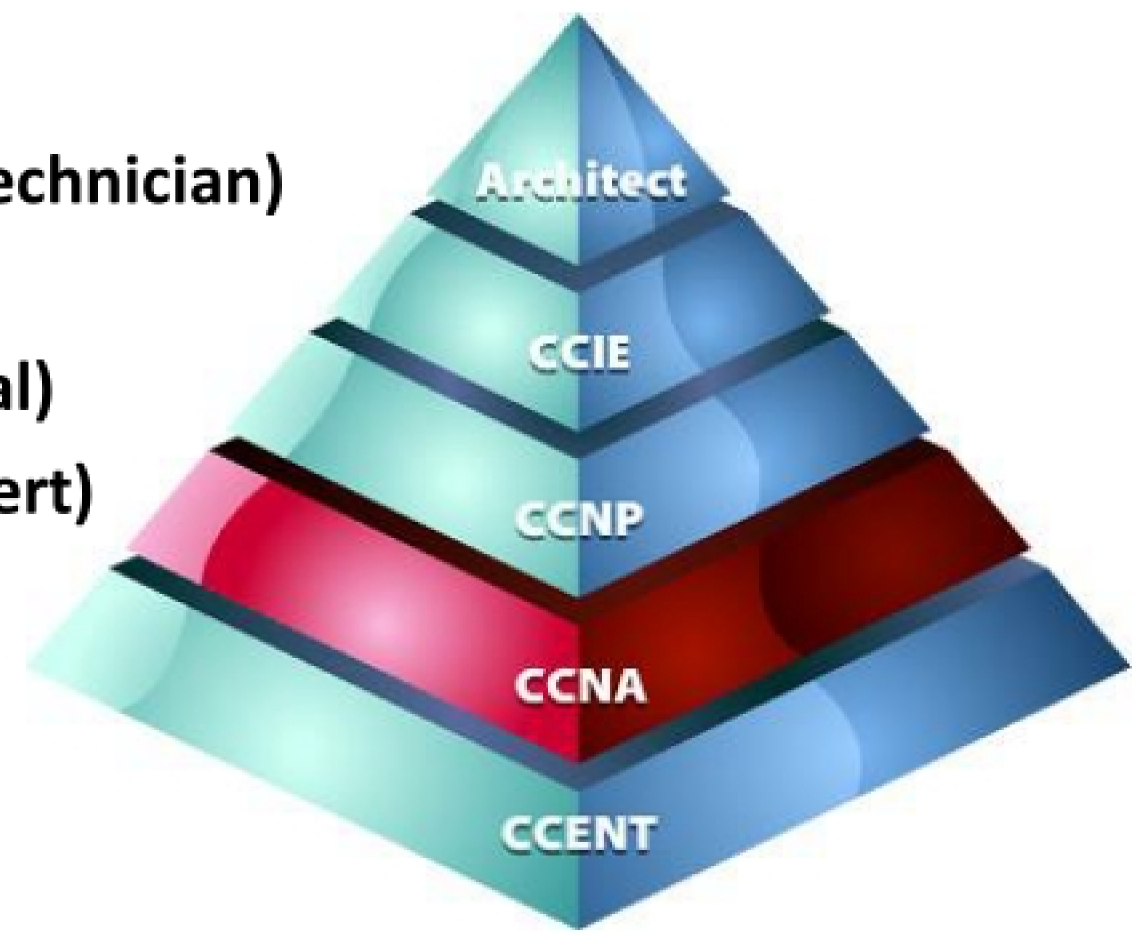
Course Presentation


Cisco Certified Network Associate
(CCNA v3.0)
ZOOM
TECHNOLOGIES


Introduction to Cisco Certifications
ZOOM
TECHNOLOGIES

CERTIFICATIONS

- Cisco certifications are globally respected IT certification programs for Wide Area Networking (Internetworking).
- Cisco has five levels of certification:
  - CCENT (Cisco Certified Entry Networking Technician)
  - CCNA (Cisco Certified Network Associate)
  - CCNP (Cisco Certified Network Professional)
  - CCIE (Cisco Certified Internetworking Expert)
  - CCAr (Cisco Certified Architect)



CCNAv3 Certification Track

- There are 2 tracks for CCNA examination :
- Two paper track
  - ICND 1 (100-105) (On passing this exam the candidate is CCENT)
  - ICND 2 (200-105) (On passing both exams the candidate is CCNA)

OR

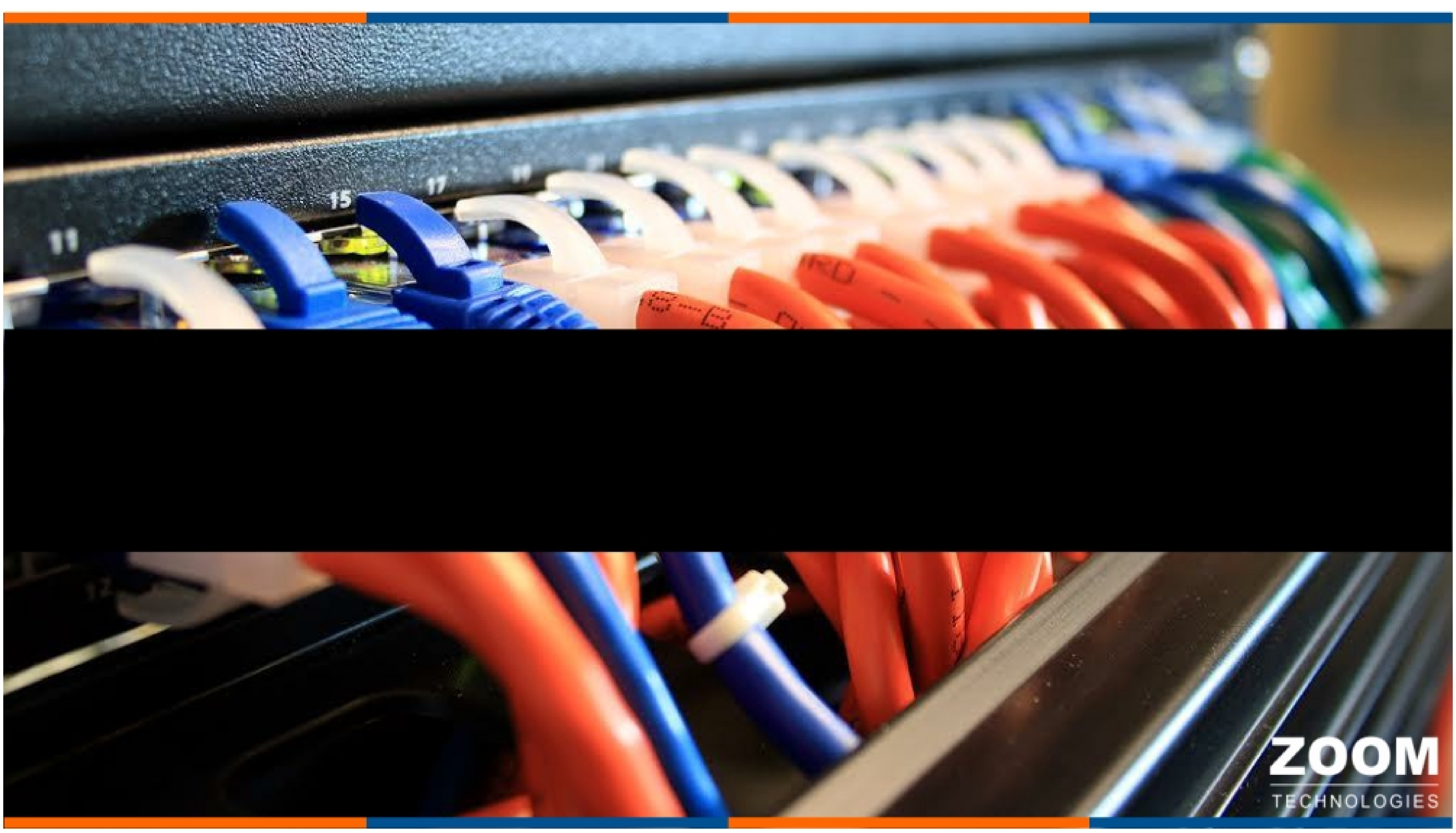
- One paper track
  - CCNA (200-125) (On passing this exam the candidate is CCNA)

CCNAv3 Certification

ZOOM TECHNOLOGIES

- Cisco Certified Network Associate R&S exam is the associate level exam into Wide Area Networking.

Exam Number	:	200-125
Duration	:	90 Minutes
Number of questions	:	50-60 questions
Passing Mark	:	825 / 1000
Available Languages	:	English
Exam Questions	:	Multiple-choice single answer
		Multiple-choice multiple answer
		Drag-and-drop
		Simulations (Simlet)
		Scenario Based (Testlet)



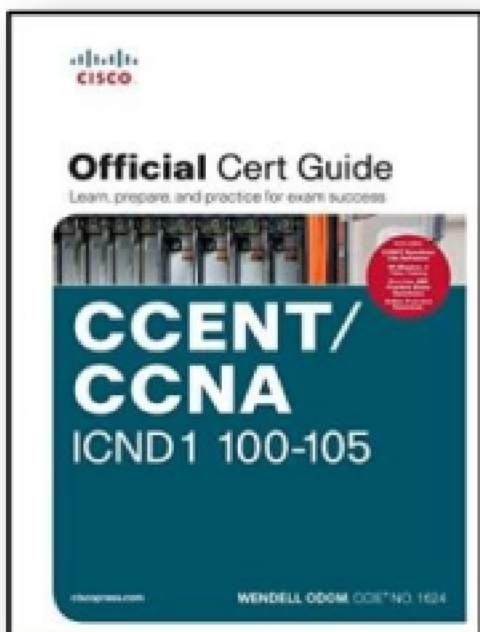
Reference Books

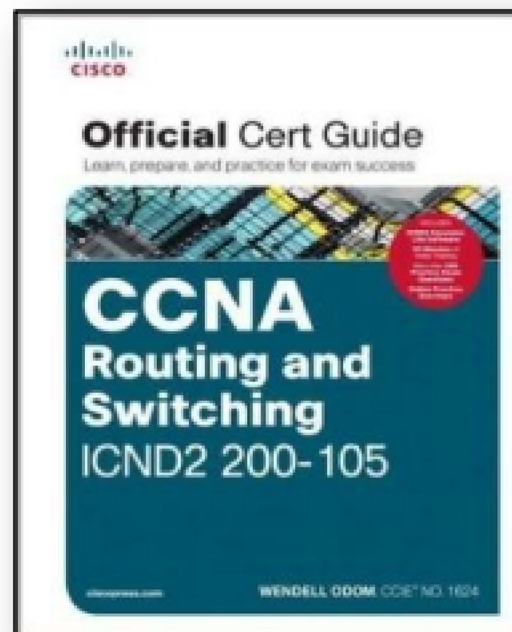
ZOOM TECHNOLOGIES

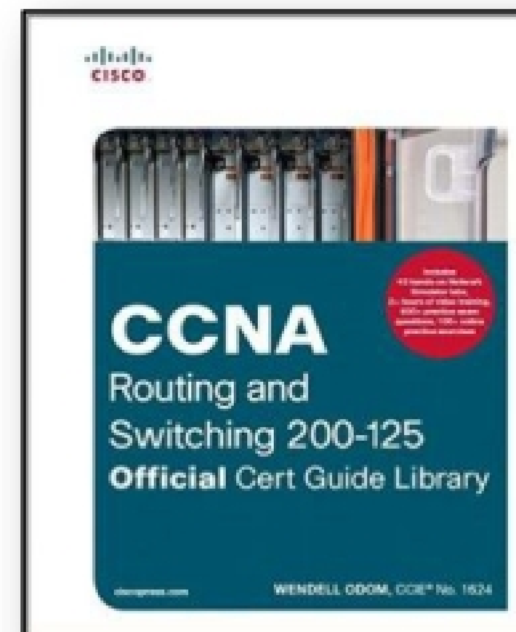
- CCNA ICND 1 (100-105) - Wendell Odom - Cisco Press
- CCNA ICND 2 (200-105) - Wendell Odom - Cisco Press

OR

- CCNA (200-125) – Wendell Odom - Cisco Press







CCIE CCNP CCNA

Day wise Schedule

ZOOM TECHNOLOGIES

DAY	TOPIC
1	Basics of Networking
2	IP Addressing - IPv4
3	IP Addressing - IPv6 and OSI layers
4	External & Internal Components of Router
5	Initial configuration of Router for IPv4 & IPv6 Network
6	WAN Connectivity and Configuration
7	Subnetting (FLSM, VLSM)
8	Introduction to Routing and Static Routing for IPv4 & IPv6 Network
9	Introduction to Dynamic Routing and RIP for IPv4 & IPv6 Network
10	OSPF - Single Area for IPv4 & IPv6 Network
11	OSPF - Multiple Area for IPv4 Network and EIGRP for IPv4 Network
12	EIGRP for IPv6 Network

Basic of Networking

Basic of Router and Router Connectivity

Routing

CCIE CCNP CCNA

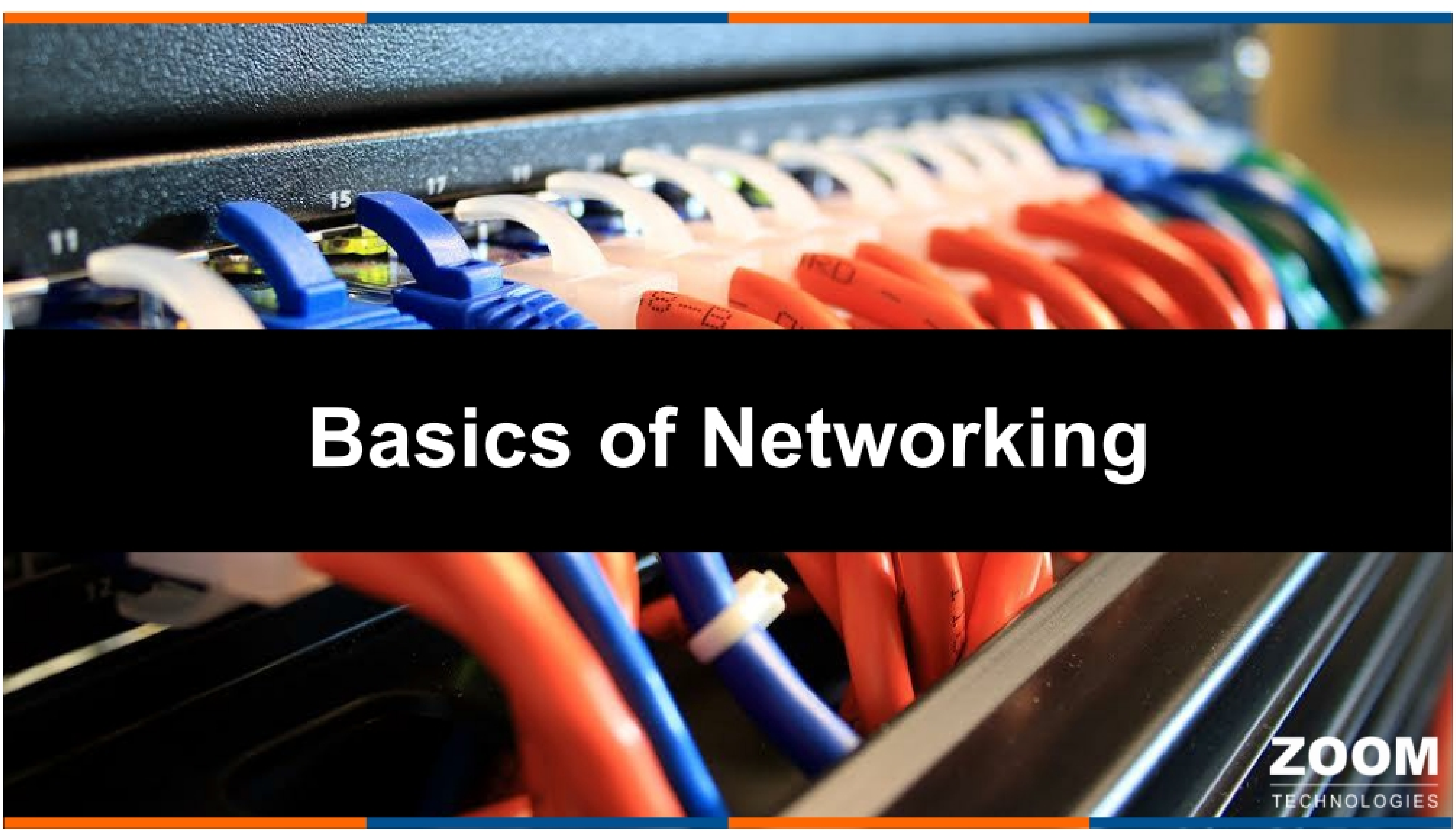
Day wise Schedule

DAY	TOPIC
13	Introduction to Switch, Initial configuration, Vlan &Trunking
14	DTP, VTP, Intervlan, CDP, Port Security
15	STP, Portfast, BPDU,ETHERCHANNEL & SPAN
16	Access Control List - IPv4
17	Access Control List - IPv6
18	Default Routing and NAT
19	HSRP, IP SLA & EBGP
20	LOCAL AUTHENTICATION, AAA, SSH and VPN
21	Syslog, NTP, SNMP, DHCP, IPv6
22	Password Recovery and Backup of IOS with TFTP, SCP, FTP
23	PPP Authentication and PPPoE
24	Live setup and Q&A

Switching

Security

Network Services
and
Advance Concepts



Network

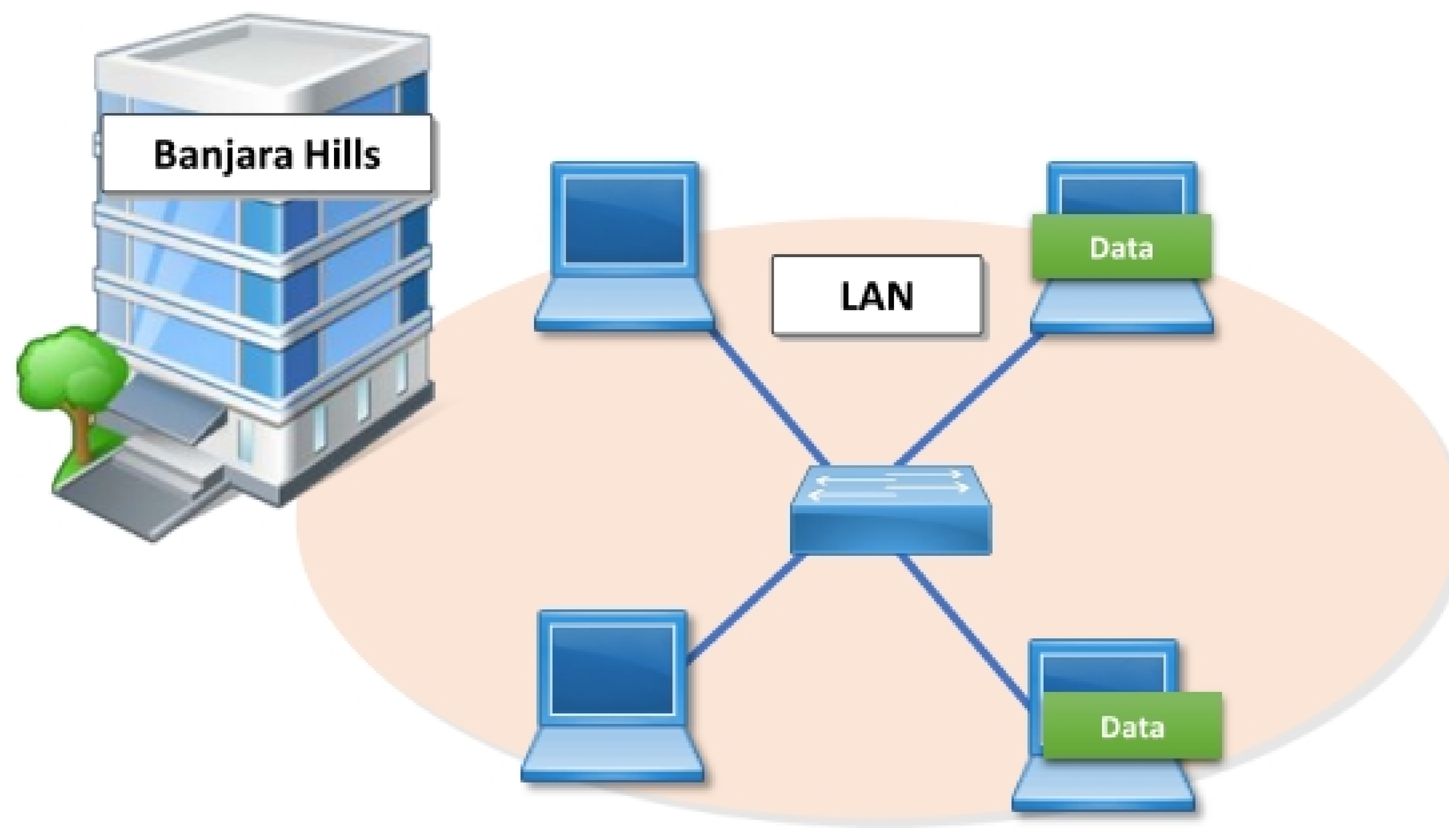
- Interconnection of two or more devices is called as a network.
- The communication between two or more interconnected devices is called networking.
- Establishing connectivity between devices with the help of Hub / Switch / Access Point for Data Communication.

Types of Networks

- LAN - Local Area Network
- MAN - Metropolitan Area Network
- WAN - Wide Area Network

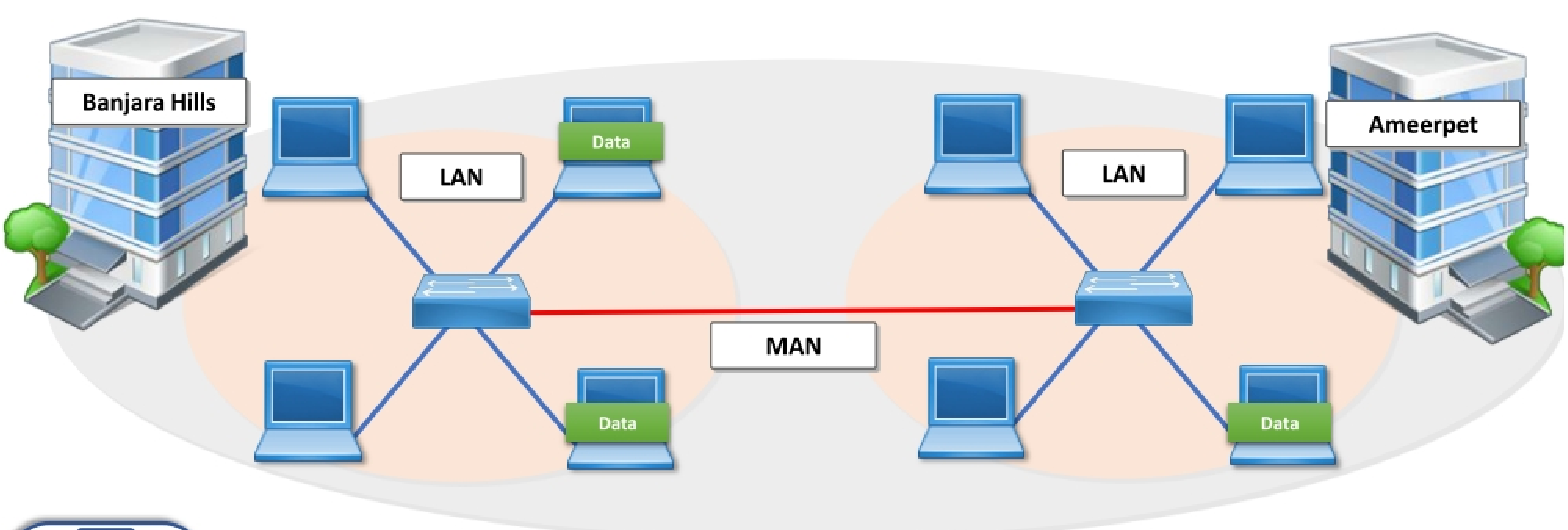
LAN

- **Local Area Networks are used to connect Interconnection of PCs and other Network devices that are very close together in a limited area such as a floor of a building, a building itself or within a campus.**



MAN

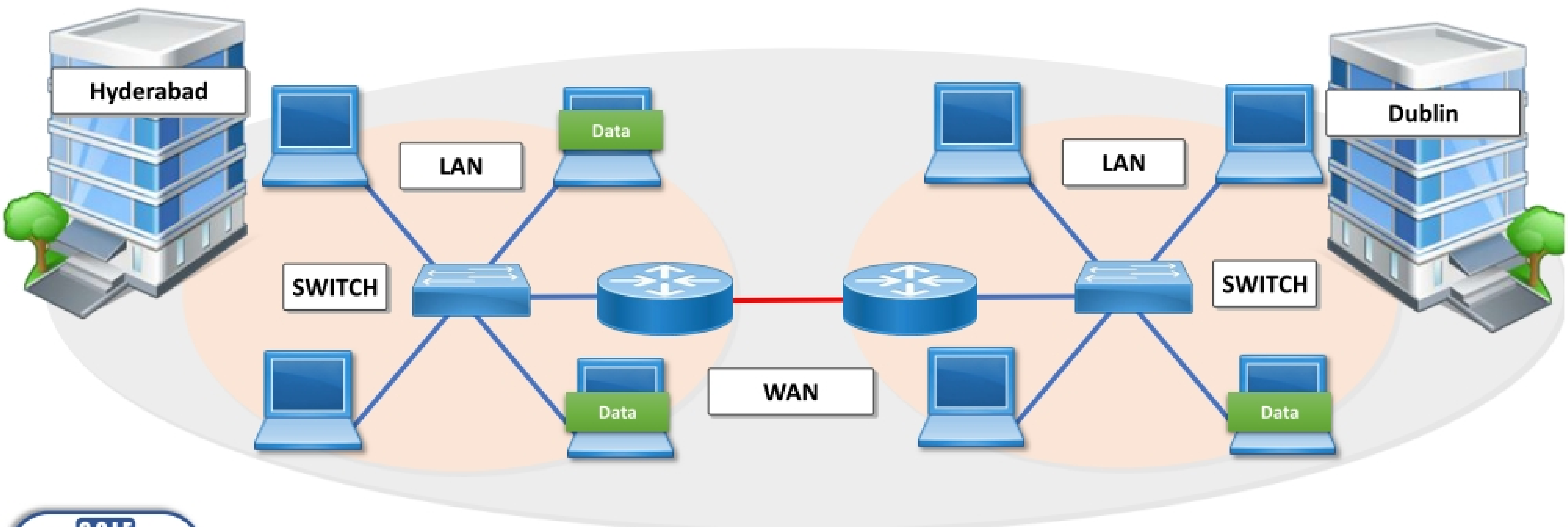
- **Metropolitan Area Network are used to connect networking devices that may span around the entire city.**



WAN

ZOOM TECHNOLOGIES

- **Wide Area Networks which connects two or more LANs present at different geographical locations.**

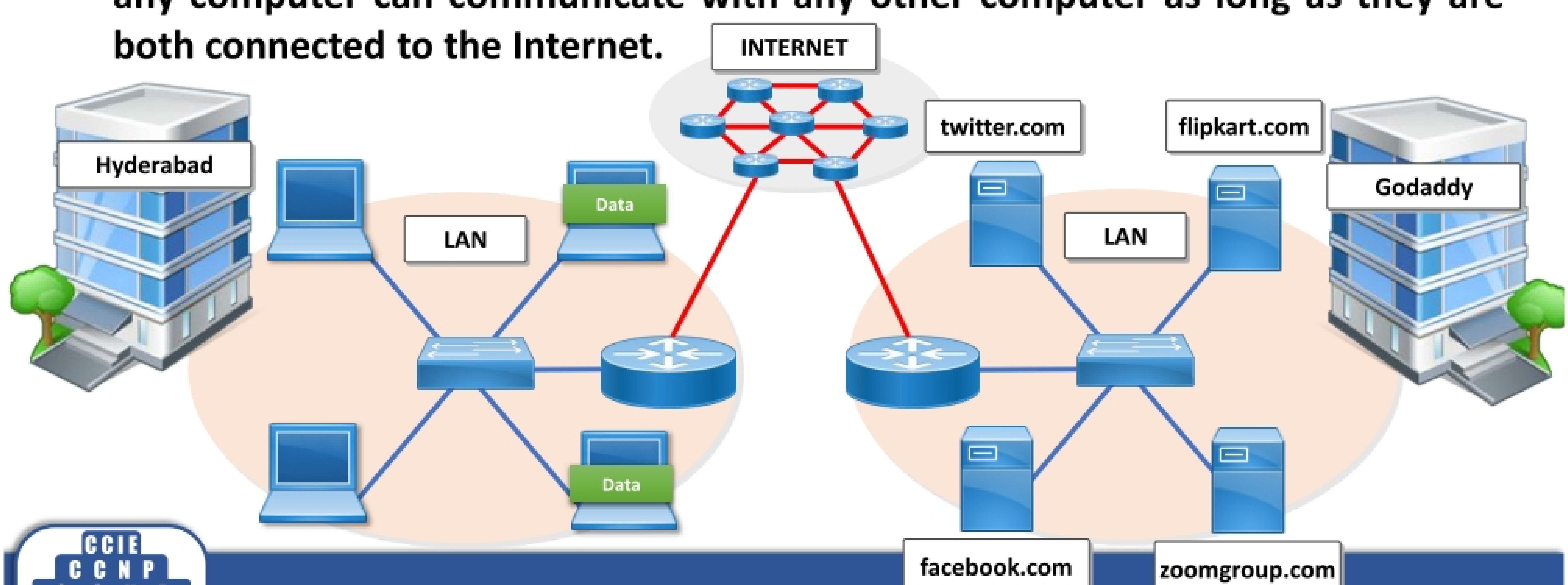


CCIE CCNP CCNA

Internet

ZOOM TECHNOLOGIES

- **Internet is a massive network of networks, a networking infrastructure.**
- **It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet.**

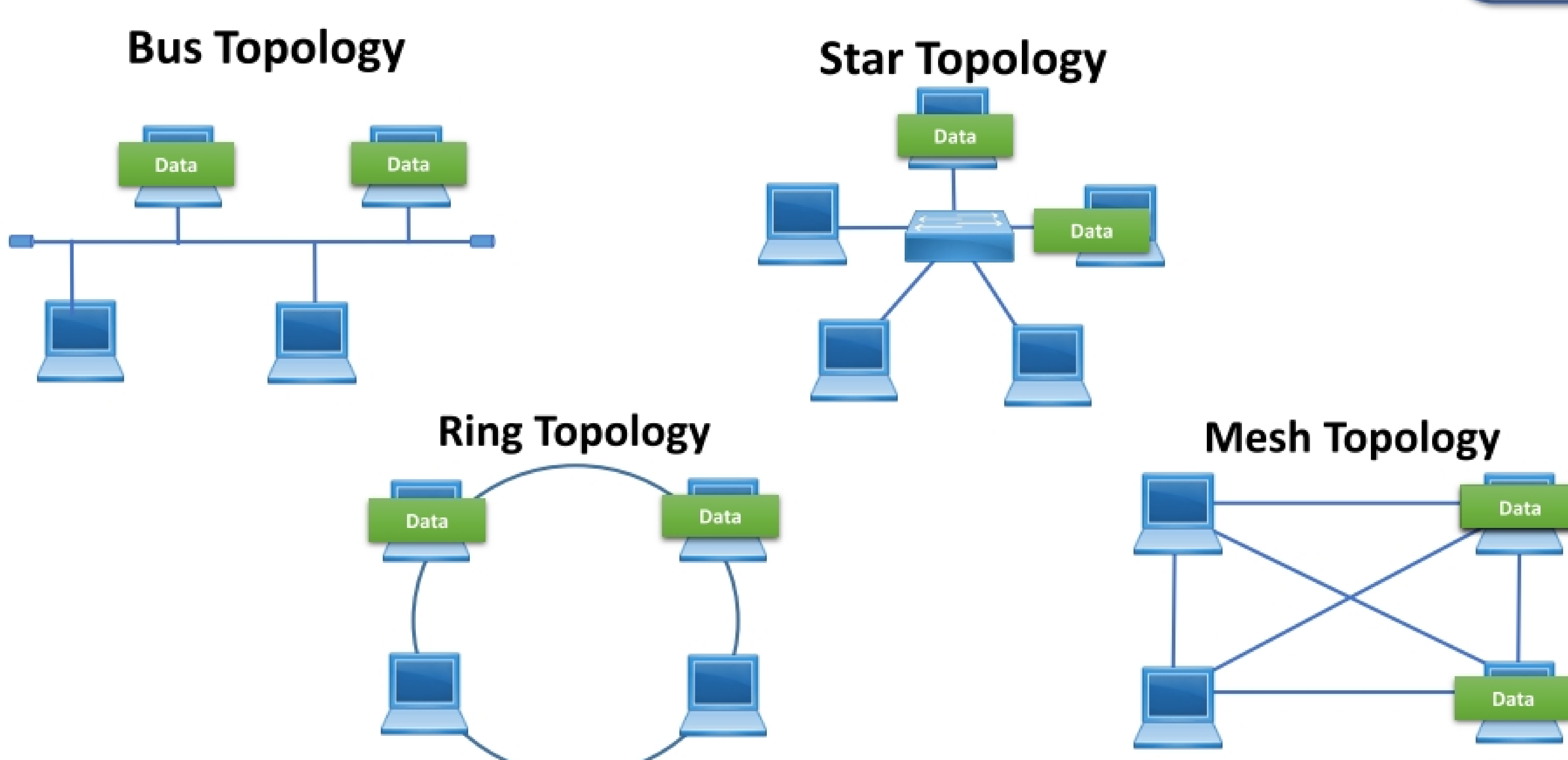


CCIE CCNP CCNA

Network Topology

- Bus Topology
- Ring Topology
- Star Topology
- Mesh Topology

Network Topology

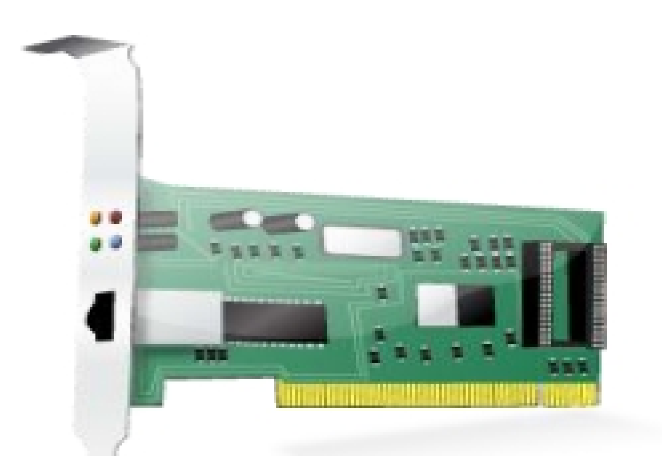


Setting up a Network

- Network Interface Card
- Media
- Network Devices

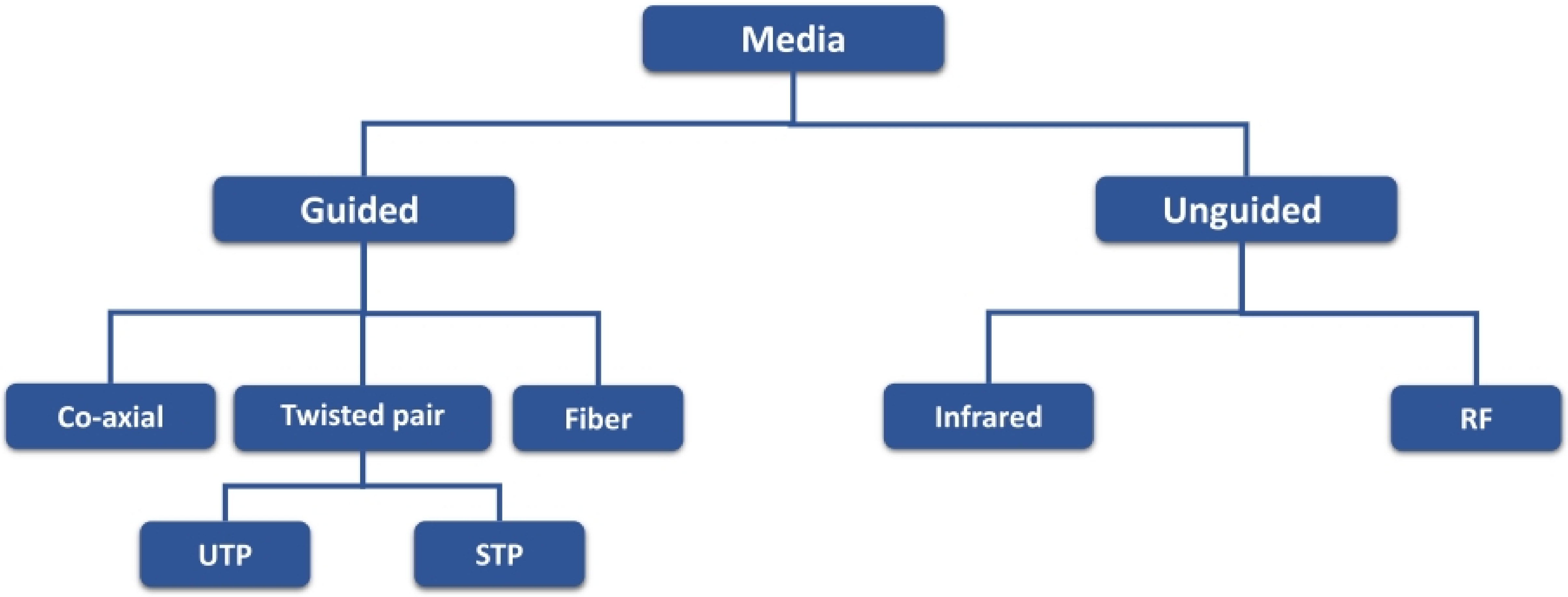
Network Interface Card (NIC)

- NIC is the interface between the computer and the network
- It is also known as the Lan card or Ethernet card
- Ethernet cards have a unique 48 bit address called as MAC (Media access control) address
  - MAC address is also called as Physical address or hardware address
  - The 48 bit MAC address is represented as 12 Hexa-decimal digits
  - Example: 0016.D3FC.603F
- Network cards are available in different speeds
  - Ethernet (10 Mbps)
  - Fast Ethernet (100 Mbps)
  - Gigabit Ethernet (1000 Mbps)



Media

- The purpose of the media is to transport bits from one machine to another.



Media

UTP Cable

Co-axial cable

STP Cable

Fiber optic

Types of Twisted Pair cables

Category	DTR	Purpose	Connector
CAT 5	100 Mbps	Fast Ethernet	RJ 45
CAT 5e	500 Mbps		RJ 45
CAT 6	1000 Mbps	Gigabit Ethernet	RJ 45

Networking Devices

- Switch
  - It is a hardware device that centralizes communications between wired devices connected within a LAN
- Wireless Access Point
  - It is a hardware device that centralizes communications between wireless and wired devices within a LAN
- Router
  - It is a device which enables communication between two or more different logical networks.

Network Diagram

Networking Devices

ZOOM TECHNOLOGIES

- Firewall
  - It is a device which protects the network from unauthorized access
  - It allows and denies the network traffic based upon policy configured.

Network Diagram

CCIE CCNP CCNA

LAN Cable types

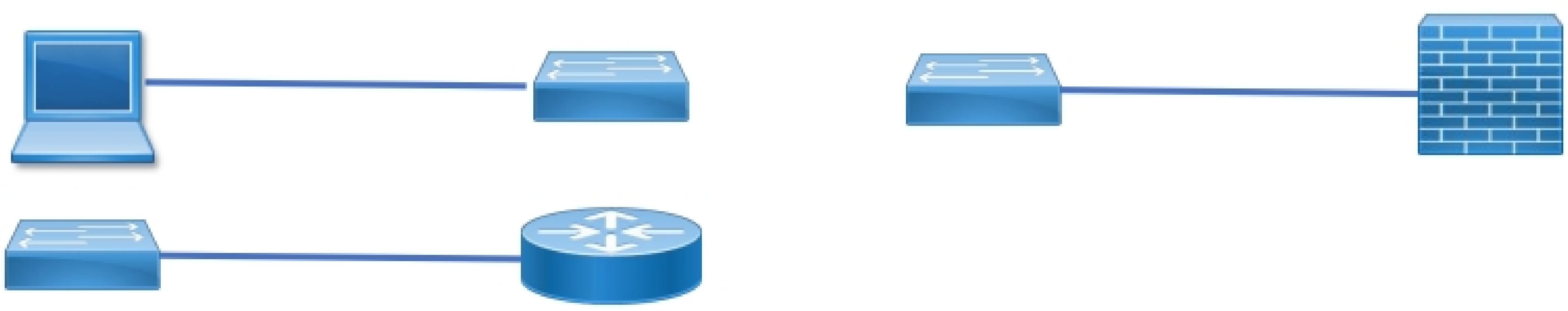
ZOOM TECHNOLOGIES

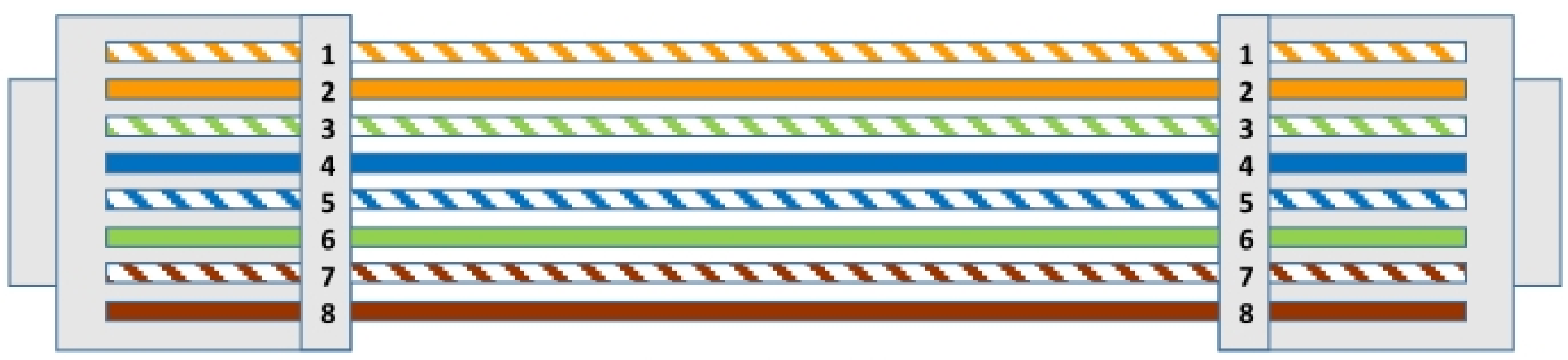
- Straight Through Cable
- Crossover Cable
- Rollover Cable

CCIE CCNP CCNA

Straight Through Cable

- **Generally used for connecting two devices of different types**



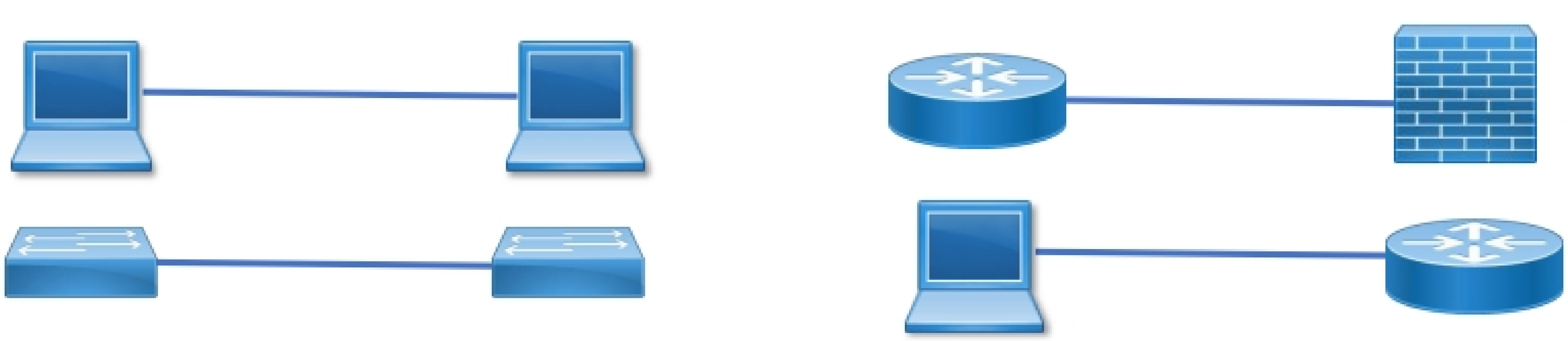


EIA/TIA 568B

Electronic Industries Alliance / Telecommunications Industry Association

Crossover Through Cable

- **Generally used for connecting same type of devices.**

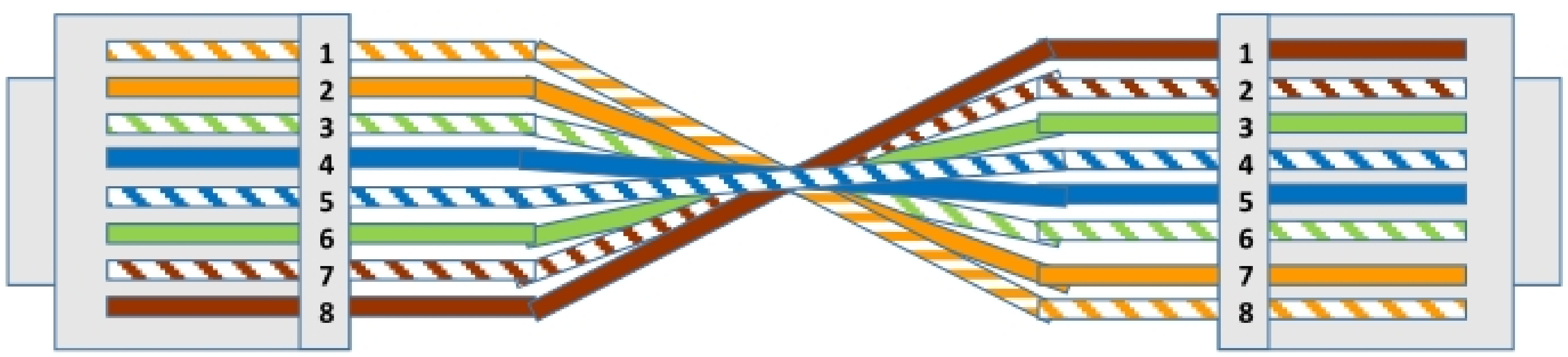


EIA/TIA 568B

Electronic Industries Alliance / Telecommunications Industry Association

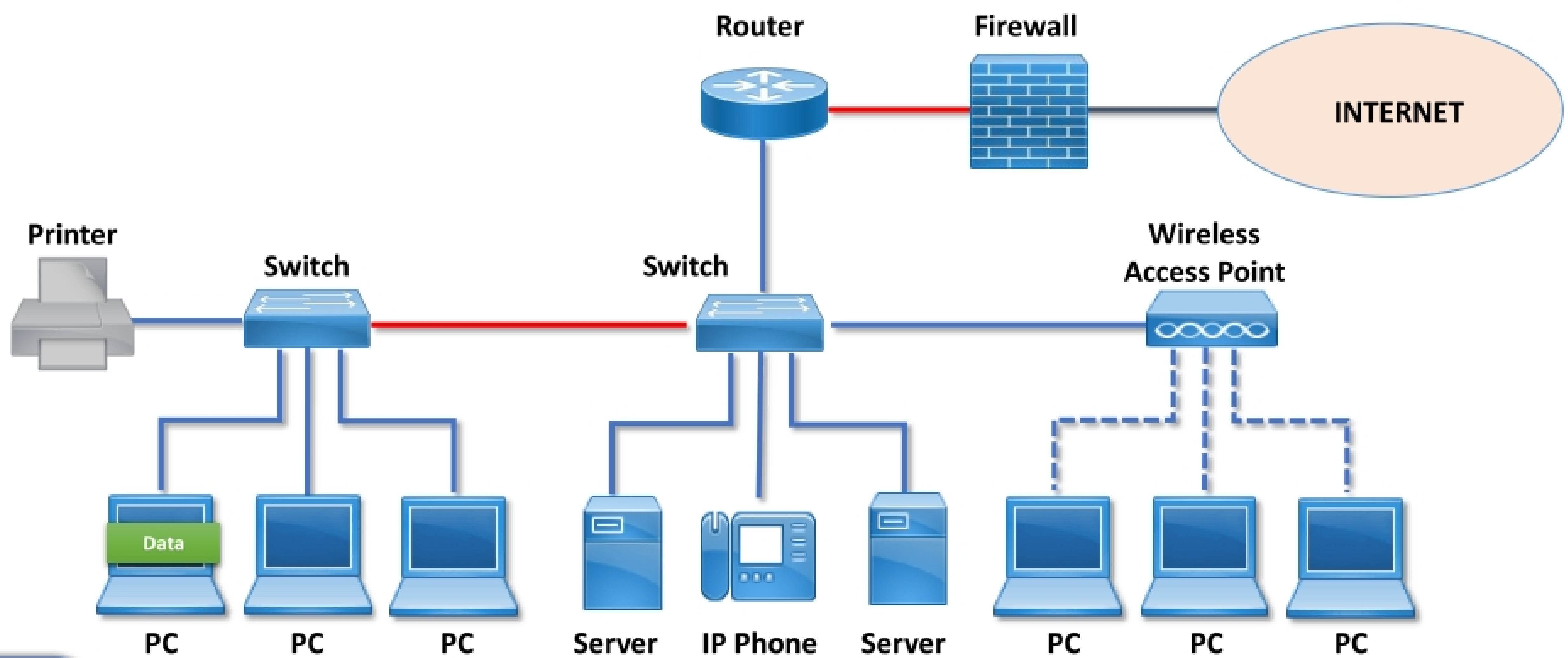
Rollover Cable

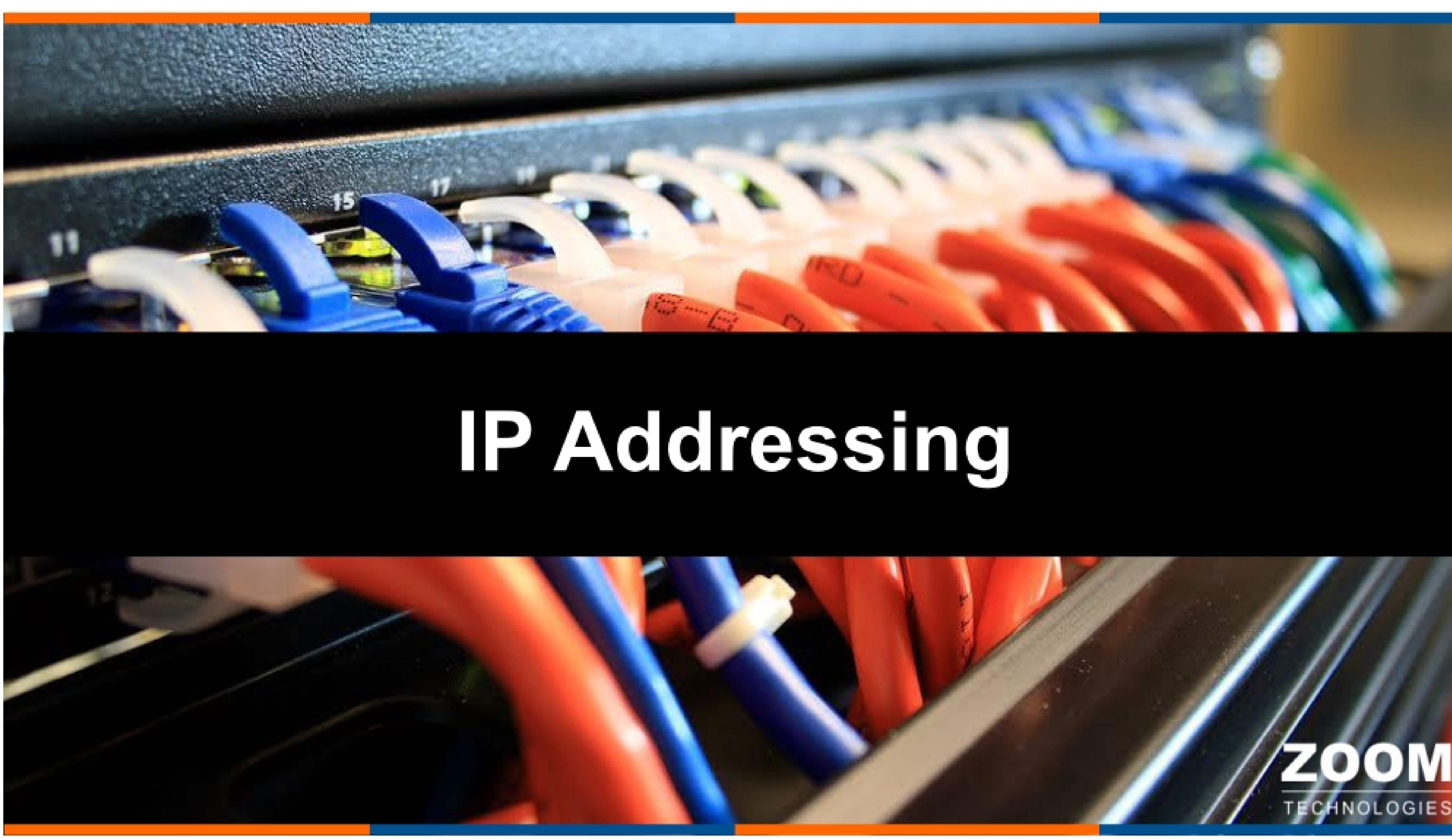
- **Generally used for connecting Router console port to Computer COM port.**



Crimping Video

Network Diagram





IP Address

- IP Address is a Logical Address
- It is a Network Layer address (Layer 3)
- Two Versions of IP:
  - IP version 4 is a 32 bit address
  - IP version 6 is a 128 bit address

IP version 4

- Bit is represent by 0 or 1 (i.e. Binary)
- IP address in binary form (32 bits):
  01010101000001011011111100000001
- 32 bits are divided into 4 Octets:

First Octet	Second Octet	Third Octet	Forth Octet
01010101.	00000101.	10111111.	00000001

- IP address in decimal form:

  85.5.191.1

IPv4 address range

Taking Example for First Octet :
Total 8 bits, Value will be 0's and 1's
i.e. 2^8 = 256 combination

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
0	0	0	0	0	0	0	0	= 0
0	0	0	0	0	0	0	1	= 1
0	0	0	0	0	0	1	0	= 2
0	0	0	0	0	0	1	1	= 3
0	0	0	0	0	1	0	0	= 4
1	1	1	1	1	1	1	1	= 255

Total IP Address Range
0 . 0 . 0 . 0
to
255.255.255.255

Binary to Decimal

128	64	32	16	8	4	2	1	Answer
1	1	0	0	0	0	0	0	192
0	0	0	0	1	0	1	0	10
1	0	1	0	1	0	0	0	168
1	0	1	0	1	1	0	0	172
0	0	0	1	0	0	0	0	16

Decimal to Binary

Decimal	128	64	32	16	8	4	2	1
18	0	0	0	1	0	0	1	0
152	1	0	0	1	1	0	0	0
200	1	1	0	0	1	0	0	0
15	0	0	0	0	1	1	1	1
240	1	1	1	1	0	0	0	0

IP Address Classification

IP address are divided into 5 Classes

- CLASS A
- CLASS B
- CLASS C

Used in LAN & WAN

- CLASS D

Reserved for Multicasting

- CLASS E

Reserved for Research & Development

Priority Bit

- Priority Bit is used for IP Address classification.
- Most significant bit(s) from the first octet are selected for Priority Bit(s).
  - Class A priority bit is **0**
  - Class B priority bits are **10**
  - Class C priority bits are **110**
  - Class D priority bits are **1110**
  - Class E priority bits are **1111**

Class A Range

- In Class A : First bit of the first octet is reserved as priority bit, bit value is zero.

0xxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
0	0	0	0	0	0	0	0	=	0
0	0	0	0	0	0	0	1	=	1
0	0	0	0	0	0	1	0	=	2
0	0	0	0	0	0	1	1	=	3
0	0	0	0	0	1	0	0	=	4
0	1	1	1	1	1	1	1	=	127

Class A Range

0 . 0 . 0 . 0 to

127 . 255 . 255 .255

Class B Range

- **In Class B : First two bits of the first octet are reserved as priority bits, bit value as 10.**

10xxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	0	0	0	0	0	0	0	=	128
1	0	0	0	0	0	0	1	=	129
1	0	0	0	0	0	1	0	=	130
1	0	0	0	0	0	1	1	=	131
1	0	0	0	0	1	0	0	=	132
1	0	1	1	1	1	1	1	=	191

Class B Range
128 . 0 . 0 . 0 to
191 . 255 . 255 .255

Class C Range

- **In Class C : First three bits of the first octet are reserved as priority bits, bit value as 110.**

110xxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	1	0	0	0	0	0	0	=	192
1	1	0	0	0	0	0	1	=	193
1	1	0	0	0	0	1	0	=	194
1	1	0	0	0	0	1	1	=	195
1	1	0	0	0	1	0	0	=	196
1	1	0	1	1	1	1	1	=	223

Class C Range
192 . 0 . 0 . 0 to
223 . 255 . 255 .255

Class D Range

- **In Class D : First four bits of the first octet are reserved as priority bits, bit value as 1110.**

1110xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	1	1	0	0	0	0	0	=	224
1	1	1	0	0	0	0	1	=	225
1	1	1	0	0	0	1	0	=	226
1	1	1	0	0	0	1	1	=	227
1	1	1	0	0	1	0	0	=	228
1	1	1	0	1	1	1	1	=	239

Class D Range
224 . 0 . 0 . 0 to
239 . 255 . 255 .255

Class E Range

- **In Class E : First four bits of the first octet are reserved as priority bits, bit value as 1111.**

1111xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	1	1	1	0	0	0	0	=	240
1	1	1	1	0	0	0	1	=	241
1	1	1	1	0	0	1	0	=	242
1	1	1	1	0	0	1	1	=	243
1	1	1	1	0	1	0	0	=	244
1	1	1	1	1	1	1	1	=	255

Class E Range
240 . 0 . 0 . 0 to
255 . 255 . 255 .255

Ranges

Class A Range
0 . 0 . 0 . 0 to
127.255.255.255

Class B Range
128 . 0 . 0 . 0 to
191.255.255.255

Class C Range
192 . 0 . 0 . 0 to
223 . 255 . 255 .255

Class D Range
224 . 0 . 0 . 0 to
239 . 255 . 255 .255

Class E Range
240 . 0 . 0 . 0 to
255 . 255 . 255 .255

Identifying Class

IP Address	Class
10.1.100.1	A
192.1.1.1	C
224.0.0.10	D
120.200.1.1	A
150.17.2.200	B
17.1.256.1	Invalid IP Address

Octet Format

- IP address is divided into Network & Host Portion
  - CLASS A is written as N.H.H.H
  - CLASS B is written as N.N.H.H
  - CLASS C is written as N.N.N.H

CLASS A – No. Networks & Hosts

- Class A Octet Format is N . H . H . H
  Network bits : 8 Host bits : 24
- No. of Networks
  = $2^{\text{no of network bits} - \text{Priority bit}}$
  = 2^{8-1} (-1 is Priority Bit for Class A)
  = 2^{7}
  = 128 – 2 (-2 is for 0 & 127 Network)
  = 126 Networks
- No. of Host
  = $2^{\text{no of host bits}} -2$
  = $2^{24} - 2$ (-2 is for Network ID & Broadcast ID)
  = 16777216 - 2
  = 16777214 Hosts/Network

CLASS B – No. Networks & Hosts

- Class B Octet Format is N . N . H . H
  Network bits : 16 Host bits : 16
- No. of Networks
  = $2^{\text{no of network bits} - \text{Priority bit}}$
  = 2^{16-2} (-2 is Priority Bit for Class B)
  = 2^{14}
  = 16384 Networks

- No. of Host
  = $2^{\text{no of host bits}}$ -2
  = $2^{16} - 2$ (-2 is for Network ID & Broadcast ID)
  = 65536 - 2
  = 65534 Hosts/Network

CLASS C – No. Networks & Hosts

- Class C Octet Format is N . N . N . H
  Network bits : 24 Host bits : 8
- No. of Networks
  = $2^{\text{no of network bits} - \text{Priority bit}}$
  = 2^{24-3} (-3 is Priority Bit for Class C)
  = 2^{21}
  = 2097152 Networks

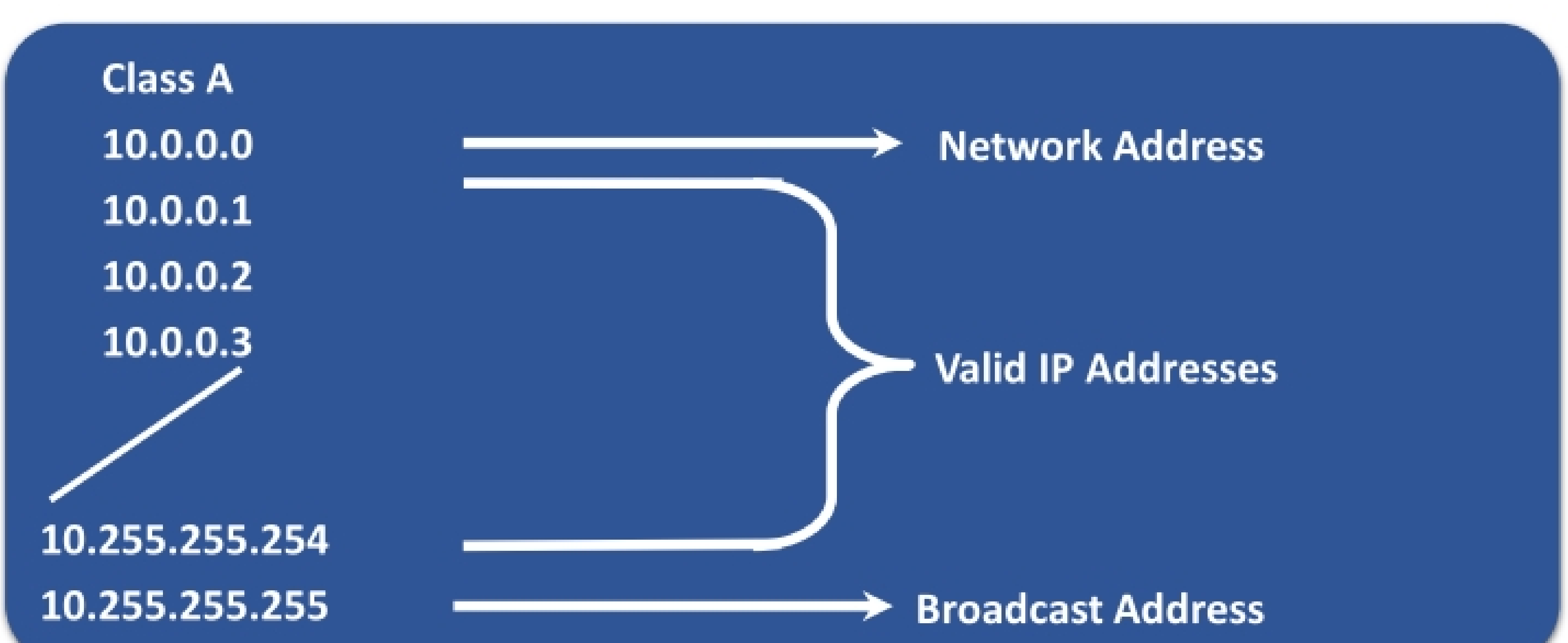
- No. of Host
  = $2^{\text{no of host bits}}$ -2
  = $2^{8} - 2$ (-2 is for Network ID & Broadcast ID)
  = 256 - 2
  = 254 Hosts/Network

Network & Broadcast Address

- Network address: IP address with all bits as ZERO in the host portion.
- Broadcast address: IP address with all bits as ONES in the host portion.
- Valid IP Addresses lie between the Network Address and the Broadcast Address.
- Only Valid IP Addresses are assigned to hosts/clients

Example - Class A

- Class A : N.H.H.H
  Network Address : 0xxxxxxx.00000000.00000000.00000000
  Broadcast Address : 0xxxxxxx.11111111.11111111.11111111



Example - Class B

- **Class B : N.N.H.H**

  Network Address : 10xxxxxx.xxxxxxxx.00000000.00000000

  Broadcast Address : 10xxxxxx.xxxxxxxx.11111111.11111111

Class B

172.16.0.0 → Network Address

172.16.0.1

172.16.0.2

172.16.0.3

172.16.255.254

(172.16.0.1 – 172.16.255.254) → Valid IP Addresses

172.16.255.255 → Broadcast Address

Example - Class C

- **Class C : N.N.N.H**

  Network Address : 110xxxxx.xxxxxxxx.xxxxxxxx.00000000

  Broadcast Address : 110xxxxx.xxxxxxxx.xxxxxxxx.11111111

Class C

192.168.1.0 → Network Address

192.168.1.1

192.168.1.2

192.168.1.3

192.168.1.254

(192.168.1.1 – 192.168.1.254) → Valid IP Addresses

192.168.1.255 → Broadcast Address

Identifying Network Address and Broadcast Address

IP Address	Network Address and Broadcast Address
120.1.1.1	120.0.0.0 and 120.255.255.255
172.16.1.1	172.16.0.0 and 172.16.255.255
10.100.1.10	10.0.0.0 and 10.255.255.255
192.168.1.10	192.168.1.0 and 192.168.1.255
150.10.1.1	150.10.0.0 and 150.10.255.255

Identifying Valid IP Address

IP Address	Valid Address
119.1.1.1	Yes
172.17.255.255	No
11.1.0.0	Yes
195.255.0.255	No
142.10.0.0	No

Subnet Mask

- Subnet Mask differentiates the Network and Host portions of an IP address
- Represented with all 1's in the network portion and with all 0's in the host portion.

Subnet Mask - Examples

- Class A : N.H.H.H

  11111111.00000000.00000000.00000000

  Default Subnet Mask for Class A is 255.0.0.0

- Class B : N.N.H.H

  11111111.11111111.00000000.00000000

  Default Subnet Mask for Class B is 255.255.0.0

- Class C : N.N.N.H

  11111111.11111111.11111111.00000000

  Default Subnet Mask for Class C is 255.255.255.0

Default subnet mask

IP Address	Default subnet mask
17.1.1.1	255.0.0.0
202.1.0.18	255.255.255.0
190.10.1.1	255.255.0.0
102.10.1.10	255.0.0.0
192.0.0.1	255.255.255.0

How Subnet Mask Works ?

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0

ANDING PROCESS :
192.168.1.1 = 11000000.10101000.00000001.00000001
255.255.255.0 = 11111111.11111111.11111111.00000000
===
192.168.1.0 = 11000000.10101000.00000001.00000000
===

- The output of an AND table is 1 if both its inputs are 1.
- For all other possible inputs the output is 0.

Private IP Address

- There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.
- These addresses are not Routable (or) valid on Internet.

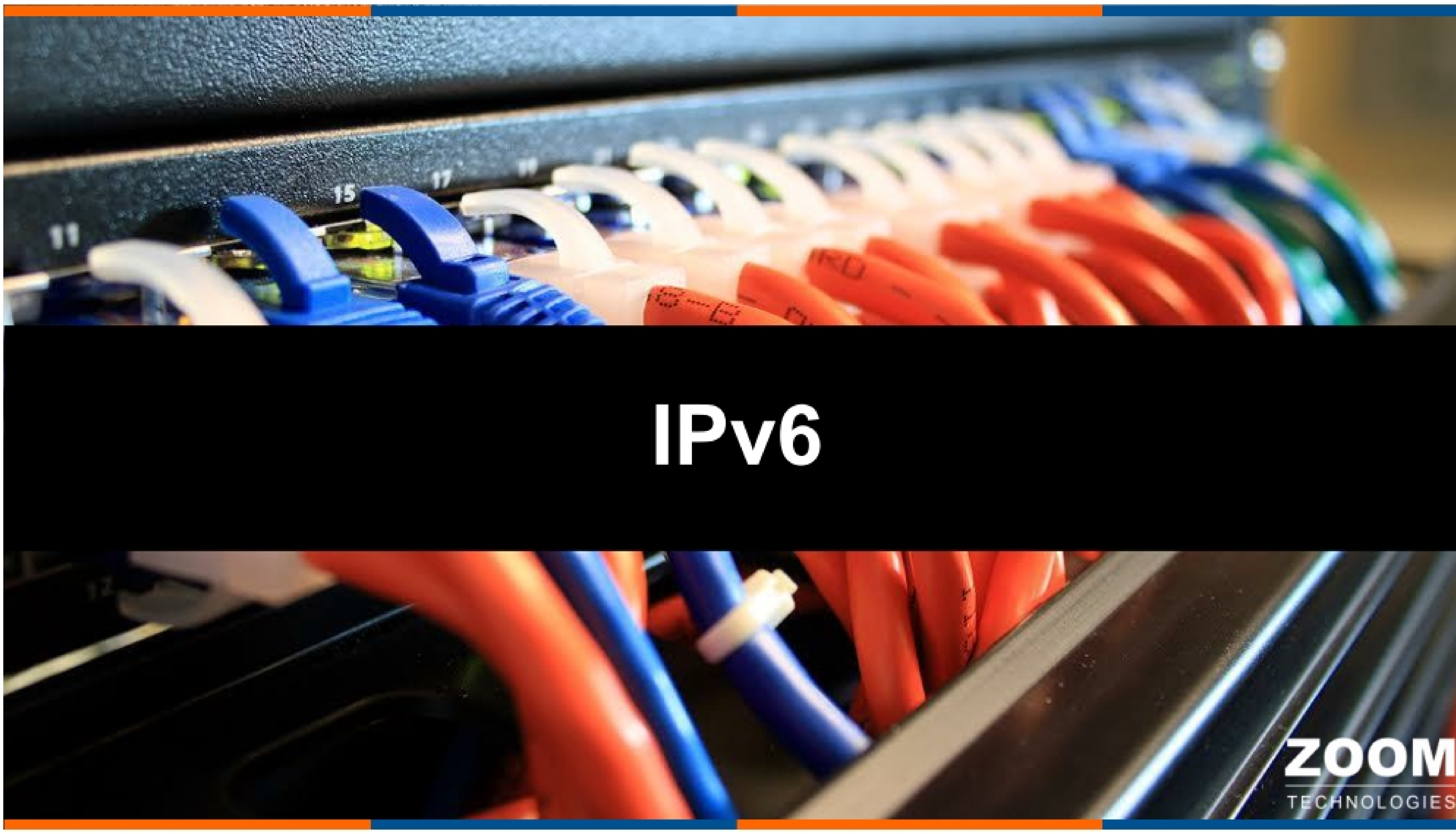
Class A
10.0.0.0 to 10.255.255.255

Class B
172.16.0.0 to 172.31.255.255

Class C
192.168.0.0 to 192.168.255.255

Public IP Address v/s Private IP Address

Public IP Address	Private IP Address
• Used on the Internet (i.e. Public Network) • It should be unique over the Internet. • Assigned by the Internet Service Provider. • Need to purchased from Internet Service Provider.	• Used within the Organization (i.e. Private Network or LAN) • It should be unique within the LAN or Organization • Assigned by Network Administrator • FREE



IPv6 Addresses

ZOOM TECHNOLOGIES

- **IPv6 is 128 bit address**
- **It is represented as 32 hexadecimal numbers arranged in 8 quartets of 4 hexadecimal digit separated by a colon " : "**

First Quartet	Second Quartet	Third Quartet	Forth Quartet	Fifth Quartet	Sixth Quartet	Seventh Quartet	Eighth Quartet
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx

xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx

- **IPv6 address in Hexadecimal form:**

  i.e. 2001:0000:0000:C15C:0000:0000:09c4:1300

- **Not case sensitive for A, B, C, D, E and F**

Binary to Hexadecimal Table

ZOOM TECHNOLOGIES

- **4 bits = 1 hex digit**

Binary				Decimal	Hexa-decimal
8	4	2	1		
0	0	0	0	0	0
0	0	0	1	1	1
0	0	1	0	2	2
0	0	1	1	3	3
0	1	0	0	4	4
0	1	0	1	5	5
0	1	1	0	6	6
0	1	1	1	7	7
1	0	0	0	8	8

Binary				Decimal	Hexa-decimal
8	4	2	1		
1	0	0	1	9	9
1	0	1	0	10	A
1	0	1	1	11	B
1	1	0	0	12	C
1	1	0	1	13	D
1	1	1	0	14	E
1	1	1	1	15	F

CCIE CCNP CCNA

Binary to Hexadecimal

ZOOM TECHNOLOGIES

Binary																Hexa-decimal
1	1	1	1													F
1	1	0	1	1	0	1	1									DB
1	0	1	1	0	0	0	1	1	0	1	0					B1A
1	0	1	1	1	0	1	0	1	0	1	1	1	0	1	0	BABA
1	1	0	0	1	0	1	0	1	1	1	1	1	1	1	0	CAFE
1	1	1	1	1	0	1	0	1	1	0	0	1	1	1	0	FACE
1	1	0	0	0	0	1	1	1	1	0	1	0	1	0	1	C3D5

HEXADECIMAL CHART

CCIE CCNP CCNA

Hexadecimal to Binary

Hexa-decimal	Binary															
E	1	1	1	0												
9	1	0	0	1												
2F	0	0	1	0	1	1	1	1								
4FD	0	1	0	0	1	1	1	1	1	1	0	1				
01E8	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	0
2001	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
FE80	1	1	1	1	1	1	1	0	1	0	0	0	0	0	0	0

HEXADECIMAL CHART

Rules for representing of IPv6 Address

- Omission of ZEROs
  - Leading zero in any quartet can be omitted.
  - Four successive zeros in a Quartet can be substituted by one zero.
- Replacing Successive Fields of Zeros with "::"
  - Multiple quartet with zero can be represented as :: but only once in a address

Omission of ZERO'S

IPv6 Address	IPv6 Address after Omission of ZERO'S
2001 : 0DB8 : 0001 : 1000 : 0000 : 0000 : 0ef0 : bc00	2001 : DB8 : 1 : 1000 : 0 : 0 : ef0 : bc00
2001 : 0DB8 : 010d : 000a : 00dd : c000 : e000 : 0001	2001 : DB8 : 10d : a : dd : c000 : e000 : 1
2001 : 2222 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001	2001 : 2222 : 0 : 0 : 0 : 0 : 0 : 1
20DB : C0A8 : 0101 : 0000 : 0000 : 0000 : 0000 : 0420	20DB : C0A8 : 101 : 0 : 0 : 0 : 0 : 420
2000 : 0000 : 0000 : 4DAD : 0023 : 0046 : 00BB : 0101	2000 : 0 : 0 : 4DAD : 23 : 46 : BB : 101
FF02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001	FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 1

Replacing Successive Fields of Zero's with "::"

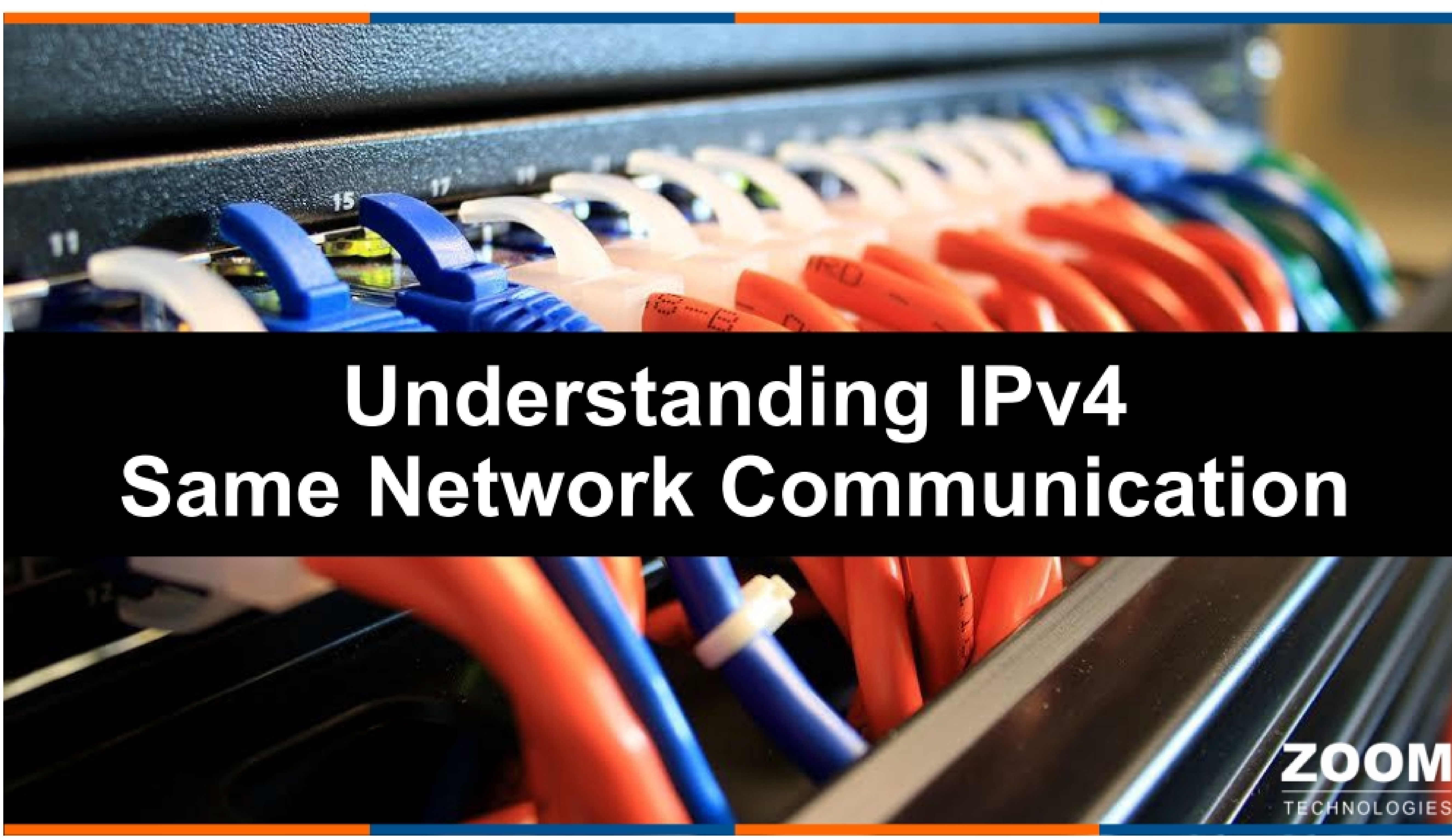
IPv6 Address	IPv6 Address after Replacing Successive Fields of Zero's with "::"
2001 : 0DB8 : 0001 : 1000 : 0000 : 0000 : 0ef0 : BC00	2001 : DB8 : 1 : 1000 : : ef0 : bc00
2002 : 1111 : 04CF : 0000 : 0000 : 0000 : 0000 : 002F	2002 : 1111 : 4CF : : 2F
3FFF : 0000 : 0000 : 0000 : 0000 : 005D : 0000 : 09CE	3FFF : : 5D : 0 : 9CE
2001 : 0000 : 0000 : FACE : B00C : 0000 : 0000 : 0069	2001 : 0 : 0 : FACE : B00C : : 69
20DB : 0000 : 0000 : 6666 : 0000 : 0000 : 0000 : 5228	20DB : 0 : 0 : 6666 : : 5228
2001 : 1111 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001	2001 : 1111 : : 1

Special Addresses (IPv4 - IPv6)

ZOOM TECHNOLOGIES

IPv6		IPv4	
Unique local	FC00::/7	Private IP address	10.0.0.0/8 172.16.0.0 to 172.31.255.255 192.168.0.0 to 192.168.255.255
Global unicast	2000::/3	Public IP address	Other Than Private IP addresses
Link local	FE80::/10	APIPA	169.254.x.x
Multicast	FF00::/8	Multicast	224.0.0.0 to 239.255.255.255
Loopback	0:0:0:0:0:0:0:1/128	Loopback	127.0.0.0/8
Default	0:0:0:0:0:0:0:0	Default	0.0.0.0

CCIE CCNP CCNA



IPv4 Same Network Communication

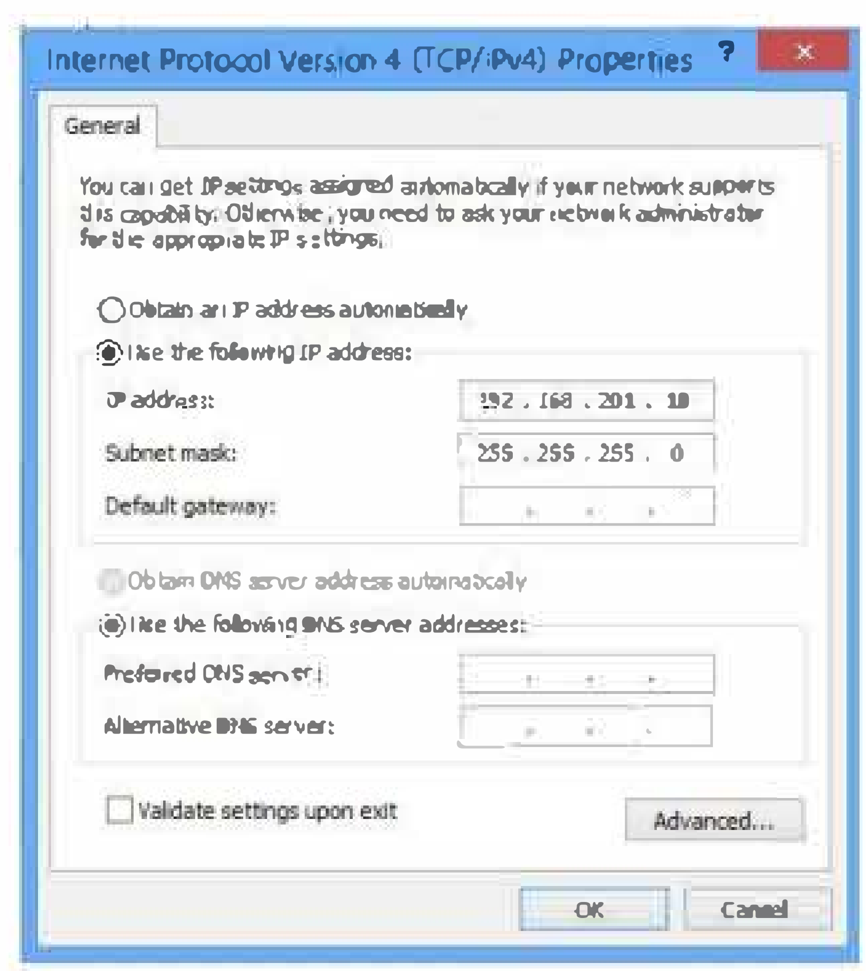
Computer	IP Address / Mask
PC-1	192.168.201.10/24
PC-2	192.168.201.20/24
PC-3	192.168.201.30/24

Computer	IP Address / Mask
PC-4	192.168.202.10/24
PC-5	192.168.202.20/24
PC-6	192.168.202.30/24

Assigning IPv4 Address on Windows Computer

On Windows 7 or Windows 8.x or Windows 10 Computer

- Open **Network and Sharing Center**
- Click on **Change adapter settings** and Click **Open.**
- Right-click on your local adapter and select **Properties.**
- In the Local Area Connection Properties window select **Internet Protocol Version 4 (TCP/IPv4)** then click the **Properties** button.
- Now select the radio button **Use the following IP address** and enter in the **IP address** and **Subnet mask** and click **OK.**



Verify IPv4 Address on Windows Computer

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix  . :
  IPv4 Address. . . . . . . . . . . . . . : 192.168.201.10
  Subnet Mask . . . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . .  :

C:\>
```

Assigning IPv4 Address on Linux Computer

```
bt ~ #  ifconfig eth0 192.168.201.10
```

Verify IPv4 Address on Linux Computer

```
bt ~ # ifconfig

eth0  Link encap:Ethernet  HWaddr 00:21:97:73:58:21
      inet addr:192.168.201.10  Bcast:192.168.201.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:171979 errors:0 dropped:0 overruns:0 frame:0
      TX packets:341932 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:12370727 (11.7 MiB)  TX bytes:463457462 (441.9 MiB)
      Interrupt:20 Base address:0xe800

lo     Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:18 errors:0 dropped:0 overruns:0 frame:0
      TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
      RX bytes:1796 (1.7 KiB)  TX bytes:1796 (1.7 KiB)
```

Ping

- **Packet Internet Groper**
- **Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network.**

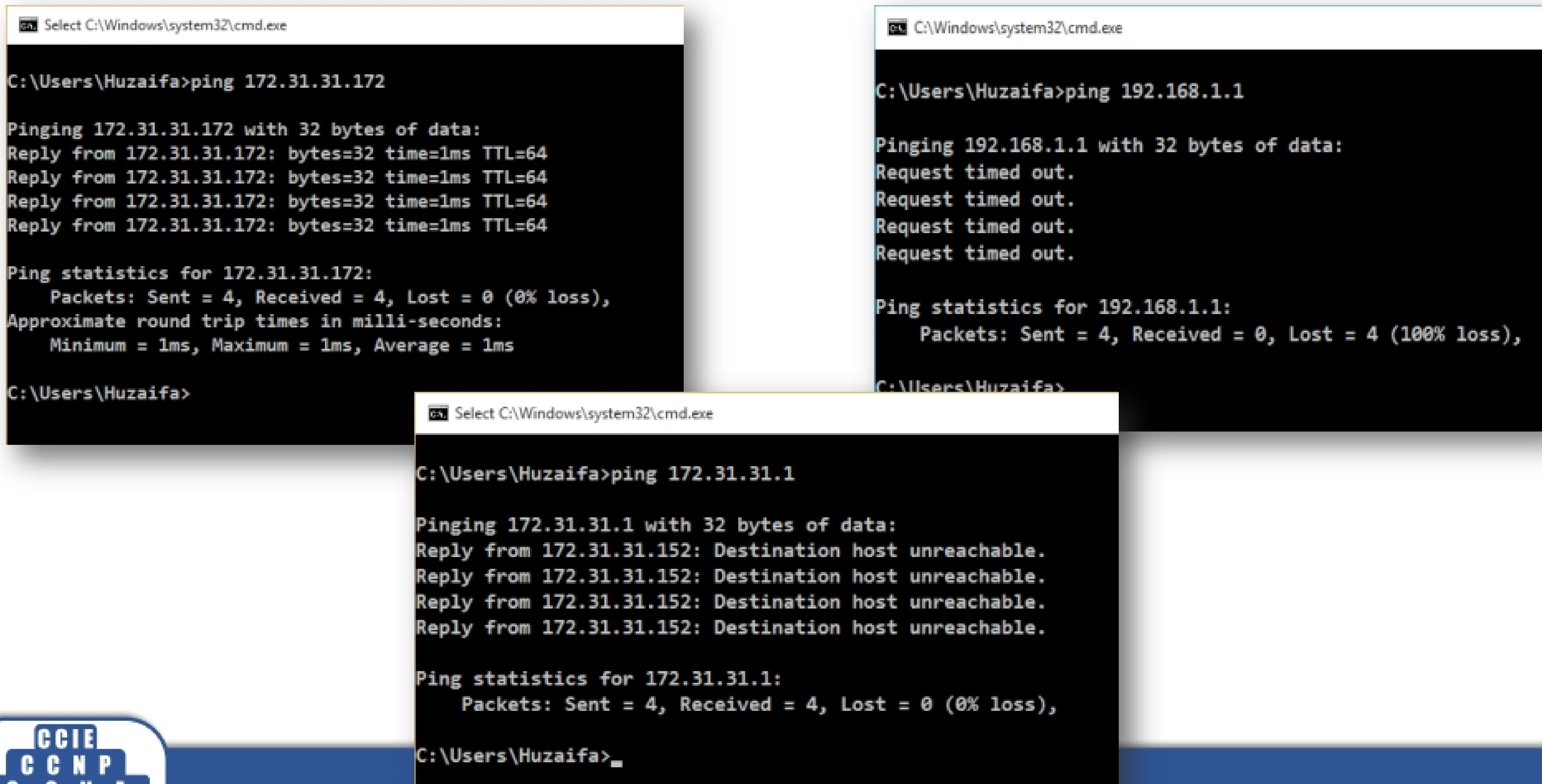
For IPv4 Network

- **Windows**
  ping 192.168.201.10
- **Linux**
  ping 192.168.201.10

For IPv6 Network

- **Windows**
  ping 2001:1111::10
- **Linux**
  ping6 2001:1111::10

PING



Select C:\Windows\system32\cmd.exe

```
C:\Users\Huzaifa>ping 172.31.31.172

Pinging 172.31.31.172 with 32 bytes of data:
Reply from 172.31.31.172: bytes=32 time=1ms TTL=64
Reply from 172.31.31.172: bytes=32 time=1ms TTL=64
Reply from 172.31.31.172: bytes=32 time=1ms TTL=64
Reply from 172.31.31.172: bytes=32 time=1ms TTL=64

Ping statistics for 172.31.31.172:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Huzaifa>
```

C:\Windows\system32\cmd.exe

```
C:\Users\Huzaifa>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Huzaifa>
```

Select C:\Windows\system32\cmd.exe

```
C:\Users\Huzaifa>ping 172.31.31.1

Pinging 172.31.31.1 with 32 bytes of data:
Reply from 172.31.31.152: Destination host unreachable.
Reply from 172.31.31.152: Destination host unreachable.
Reply from 172.31.31.152: Destination host unreachable.
Reply from 172.31.31.152: Destination host unreachable.

Ping statistics for 172.31.31.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Huzaifa>
```

Traceroute

- **Traceroute is a computer network diagnostic utility used to view the route (path) of packets across an Internet Protocol (IP) network.**

For IPv4 Network

- **Windows**

  tracert 192.168.201.10

- **Linux**

  traceroute 192.168.201.10

For IPv6 Network

- **Windows**

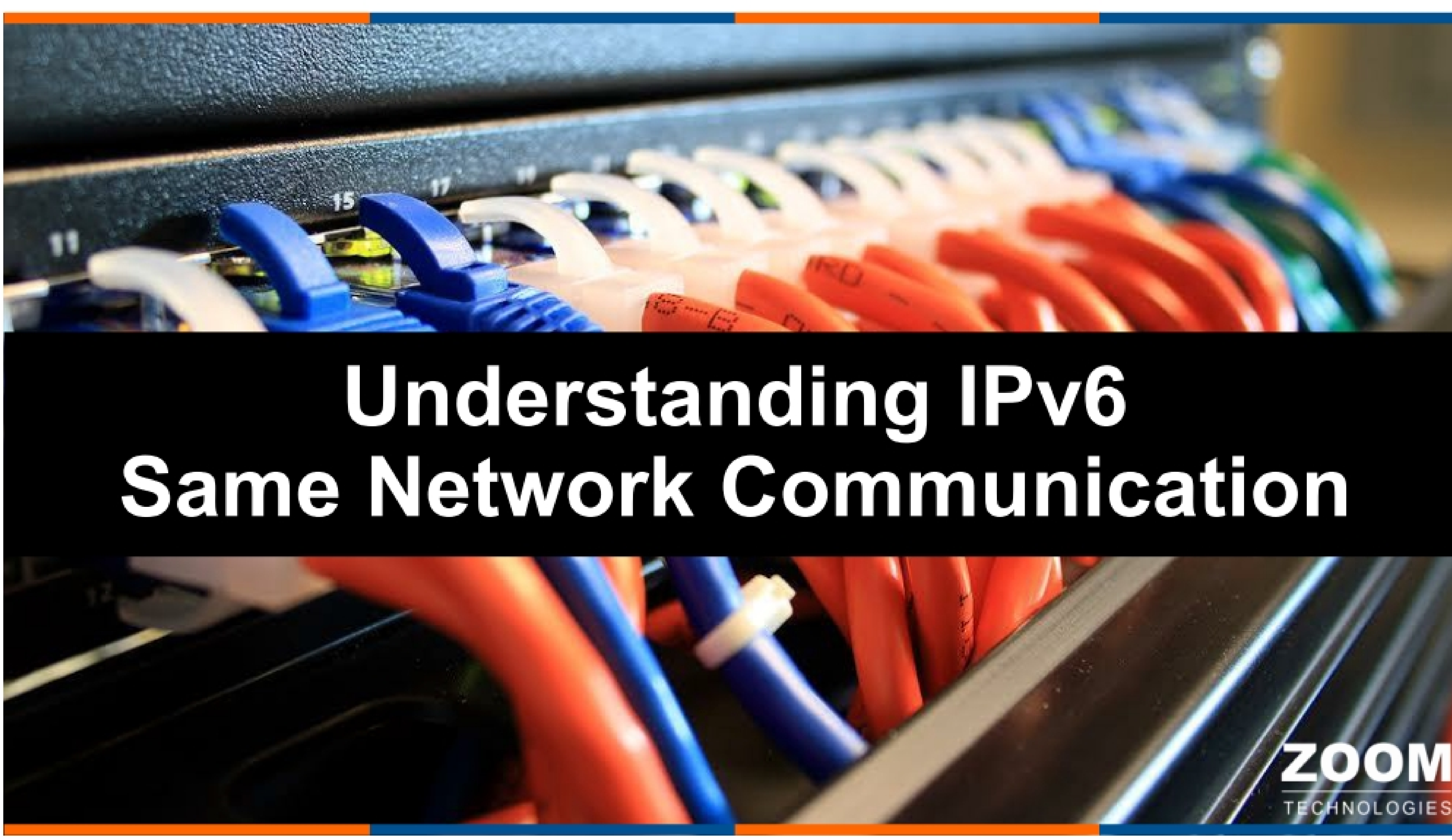
  tracert 2001:1111::10

- **Linux**

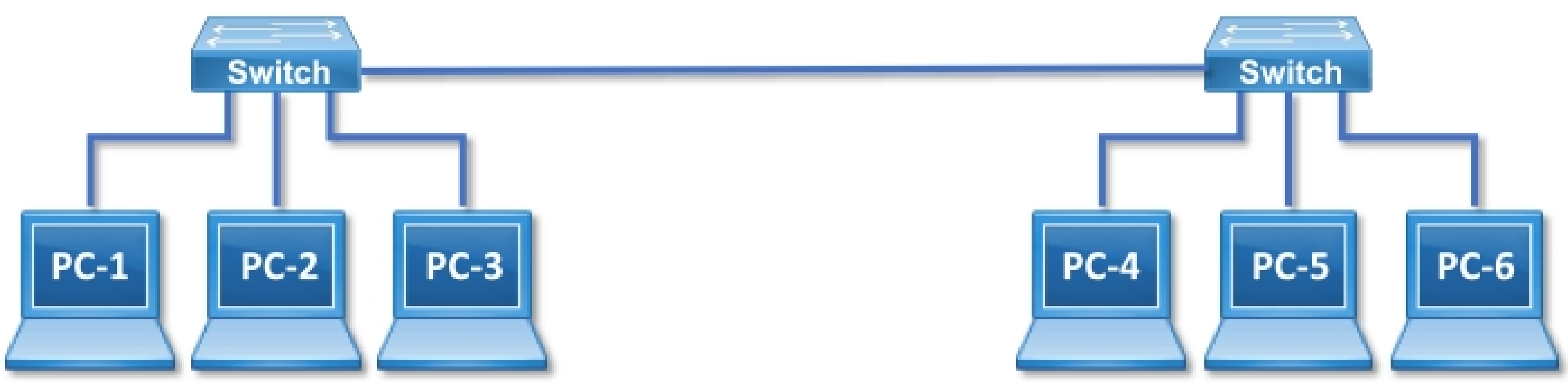
  traceroute6 2001:1111::10

Traceroute

```
C:\Windows\system32\cmd.exe

C:\Users\Huzaifa>tracert www.google.com

Tracing route to www.google.com [216.58.197.68]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  10.117.0.1
  2     2 ms     2 ms     2 ms  10.120.0.1
  3     2 ms     1 ms     3 ms  broadband.actcorp.in [183.82.14.221]
  4    31 ms    31 ms    31 ms  broadband.actcorp.in [183.82.14.93]
  5    25 ms    25 ms    25 ms  72.14.194.18
  6    17 ms    31 ms    16 ms  72.14.235.69
  7    17 ms    17 ms    17 ms  209.85.250.67
  8    25 ms    26 ms    20 ms  maa03s21-in-f4.1e100.net [216.58.197.68]

Trace complete.

C:\Users\Huzaifa>
```



IPv6 Same Network Communication



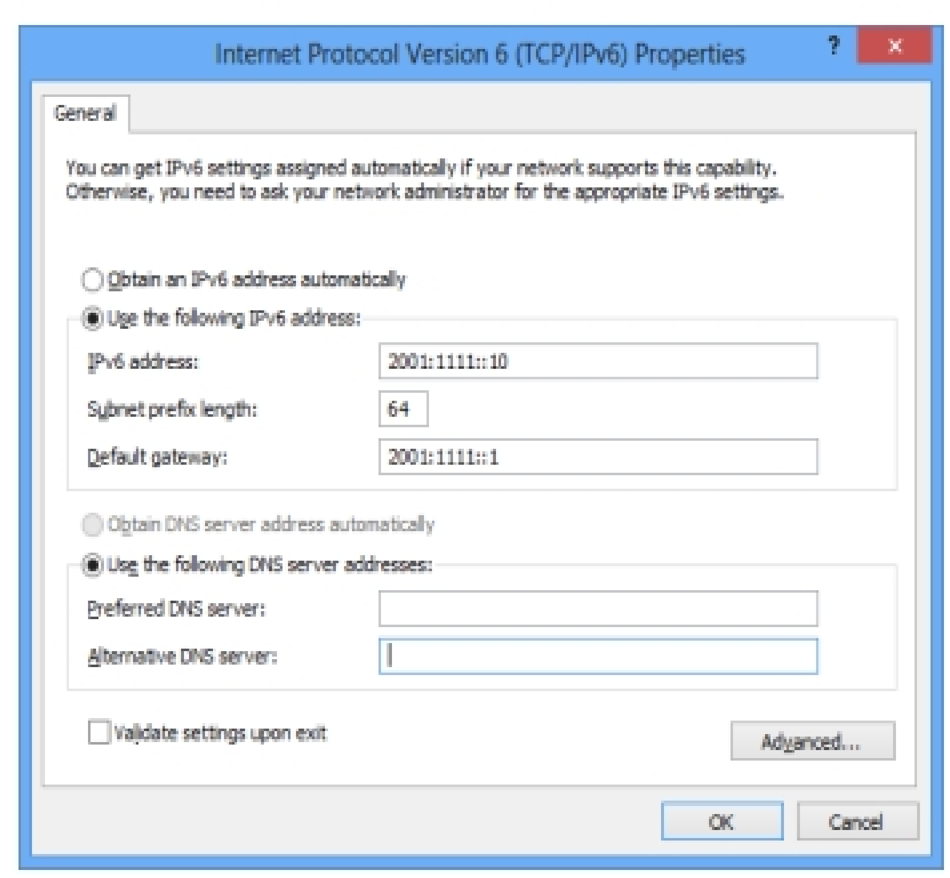
Computer	IP Address / Mask
PC-1	2001:1111::10/64
PC-2	2001:1111::20/64
PC-3	2001:1111::30/64

Computer	IP Address / Mask
PC-4	2001:2222::10/64
PC-5	2001:2222::20/64
PC-6	2001:2222::30/64

Assigning IPv6 Address on Windows Computer

On Windows 7 or Windows 8.x or Windows 10 Computer

- Open **Network and Sharing Center**
- Click on **Change adapter settings** and Click **Open**.
- Right-click on your local adapter and select **Properties**.
- In the Local Area Connection Properties window select **Internet Protocol Version 6 (TCP/IPv6)** then click the **Properties** button.
- Now select the radio button **Use the following IP address** and enter in the **IP address** and **Subnet mask** and click **OK.**



Verify IPv6 Address on Windows Computer

C:\> **ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . : **2001:1111::10**

Link-local IPv6 Address . . . . : fe80::449d:6a9a:2c80:80dc%64

Default Gateway . . . . :

C:\>

Assigning IPv6 Address on Linux Computer

bt ~ # **ifconfig eth0 inet6 add 2001:1111::10/64**

Verify IPv6 Address on Linux Computer

bt ~ # **ifconfig**

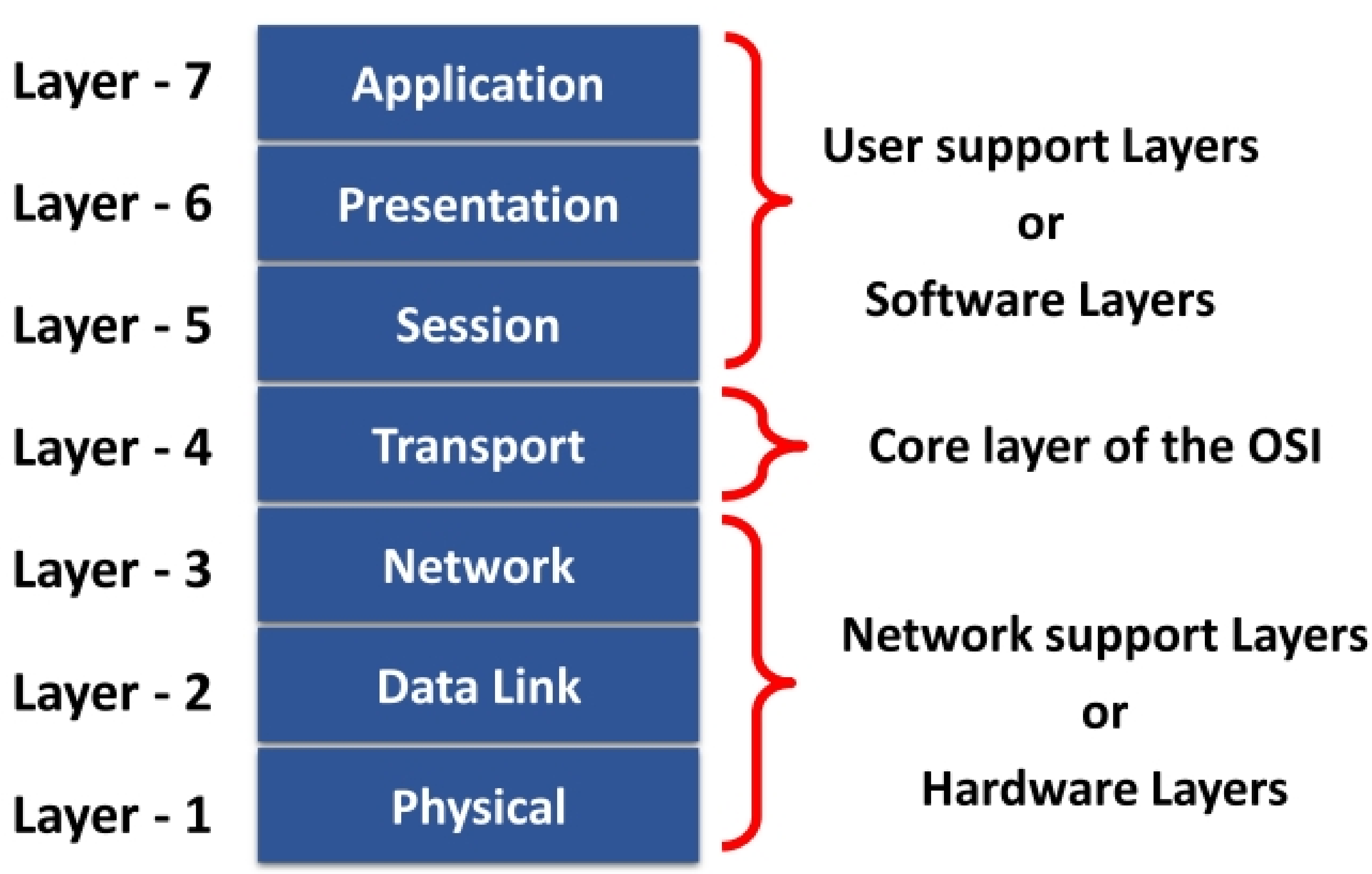
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 **2001:1111::10** prefix len **64** scopeid 0x0<global>
    ether 44:8a:5b:d4:39:3c txqueuelen 1000 (Ethernet)
    RX packets 230 bytes 82110 (80.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 121 bytes 19549 (19.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Open System Interconnect (OSI)

- OSI was developed by the International Organization for Standardization (ISO) and introduced in 1984.
- It is a layered architecture (consists of seven layers).
- Each layer defines a set of functions which takes part in data communication.

OSI Model Layers



Application Layer

- **Application**
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

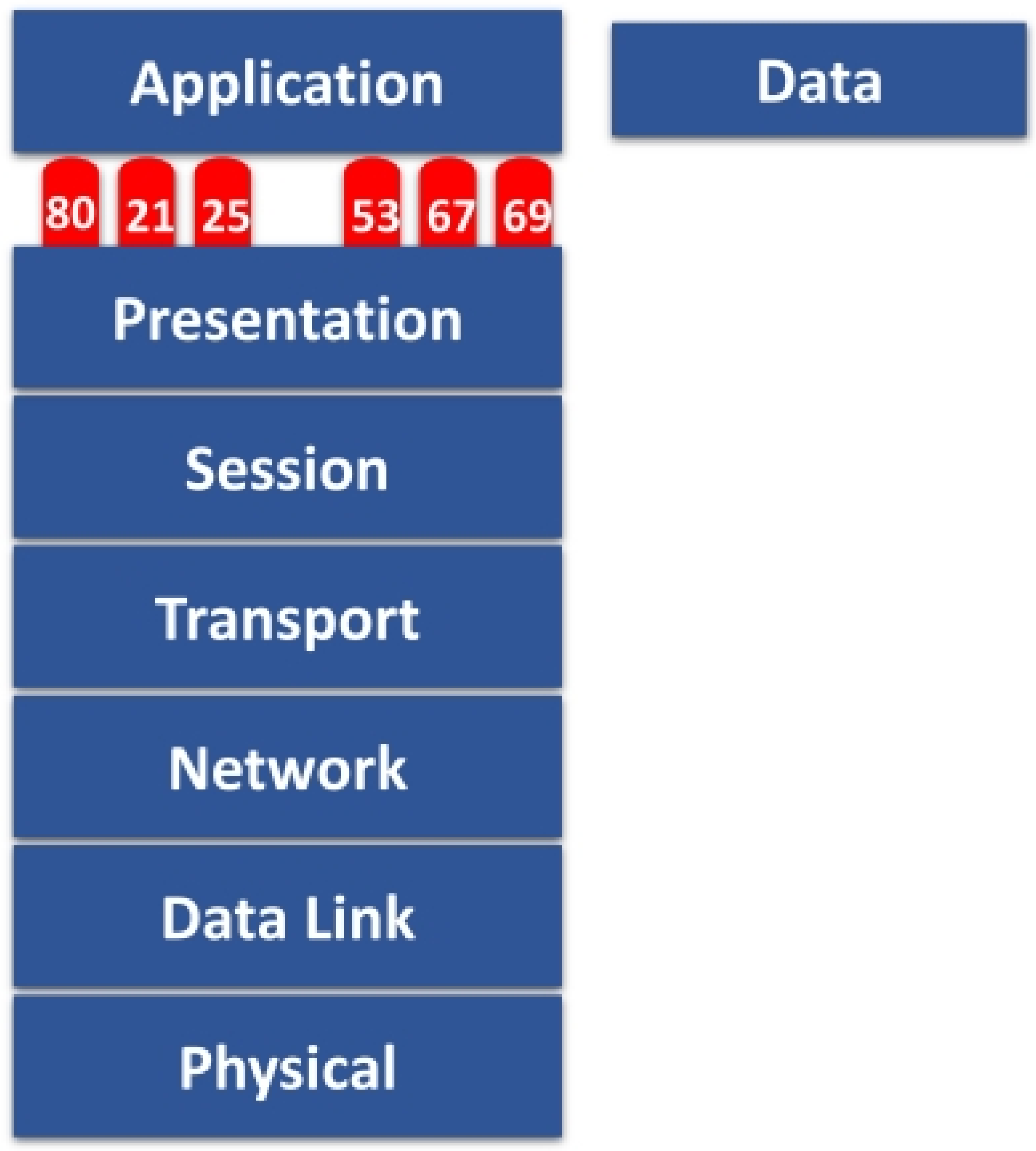
It is responsible for providing an interface for the users to interact with application services or Networking Services .

Ex: Web browser(HTTP), Telnet etc.

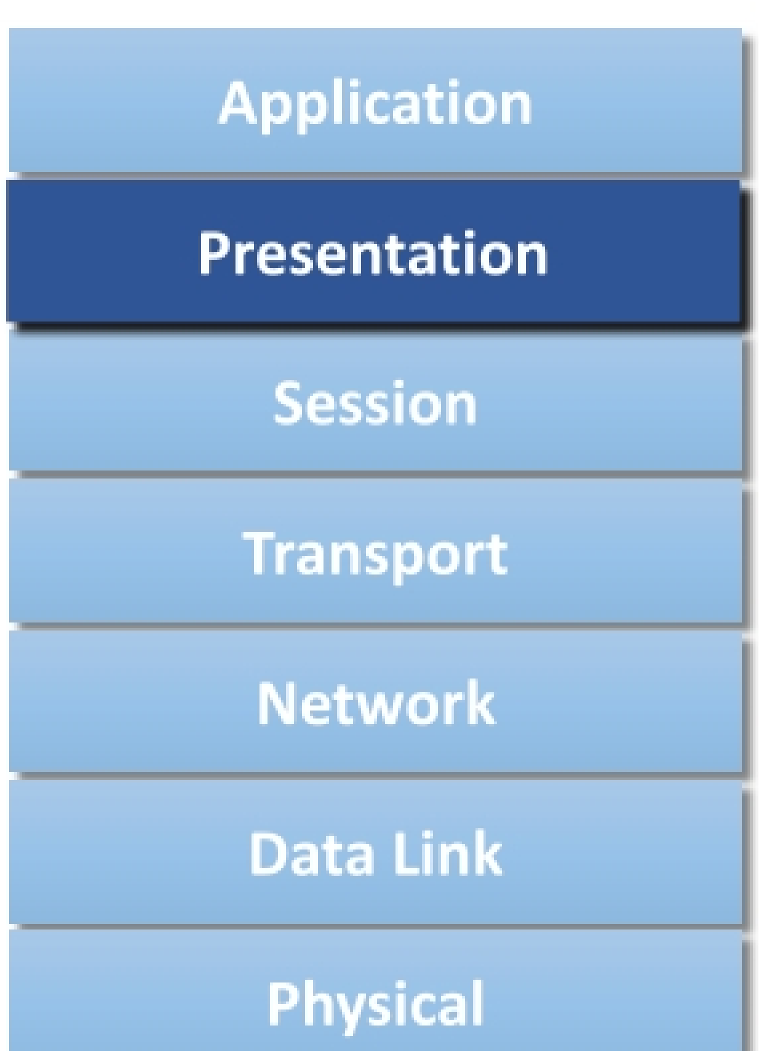
Examples of Networking Services

Service	Port No.
HTTP	80
FTP	21
SMTP	25
TELNET	23
TFTP	69

Data flow from Application Layer



Presentation Layer



It is responsible for defining a standard format to the data.

It deals with data presentation.

The major functions described at this layer are..

- Encoding – Decoding

  Ex : ASCII, EBCDIC (Text)

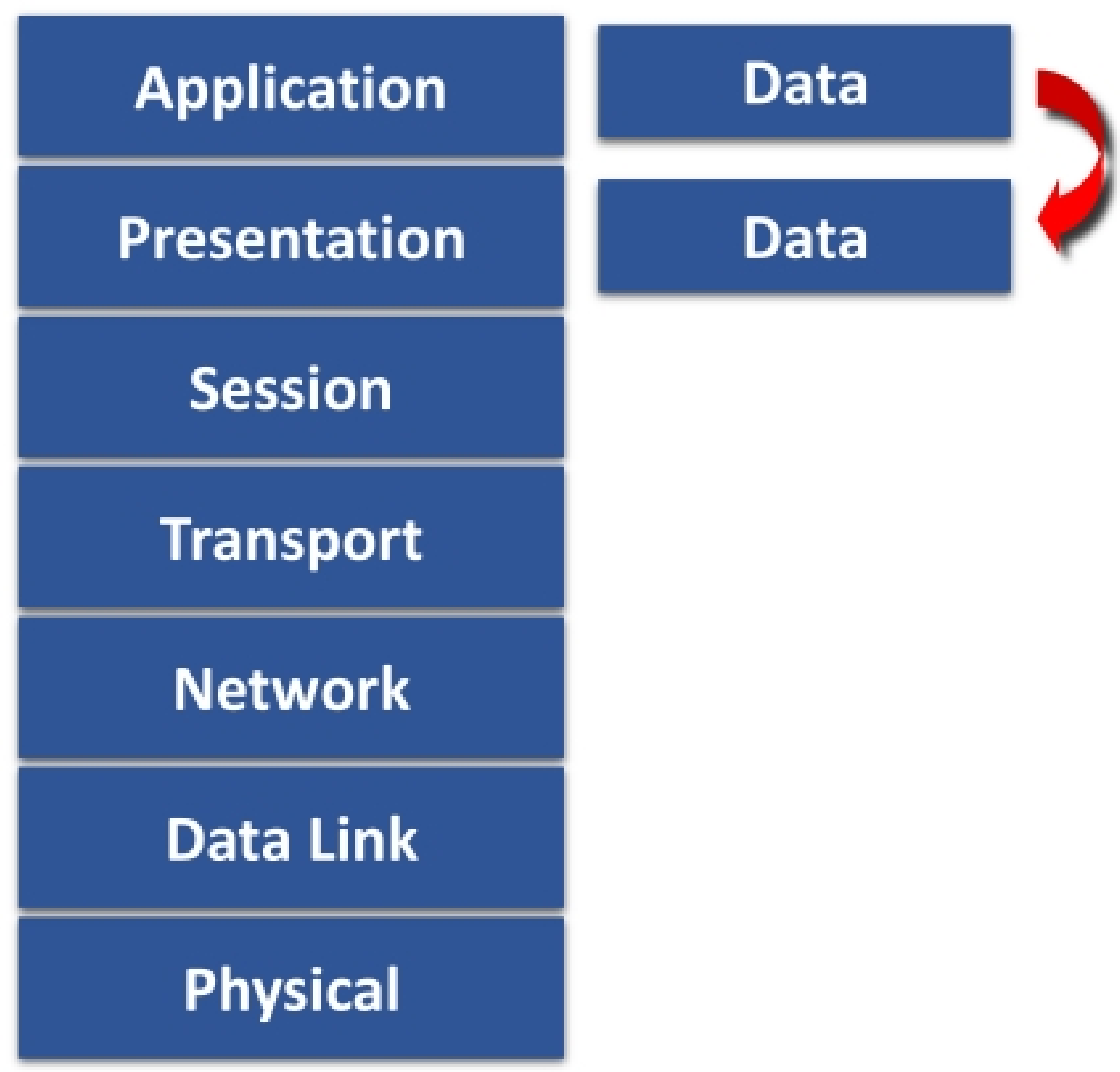
  JPEG,GIF,TIFF (Graphics)

  MIDI,WAV (Voice)

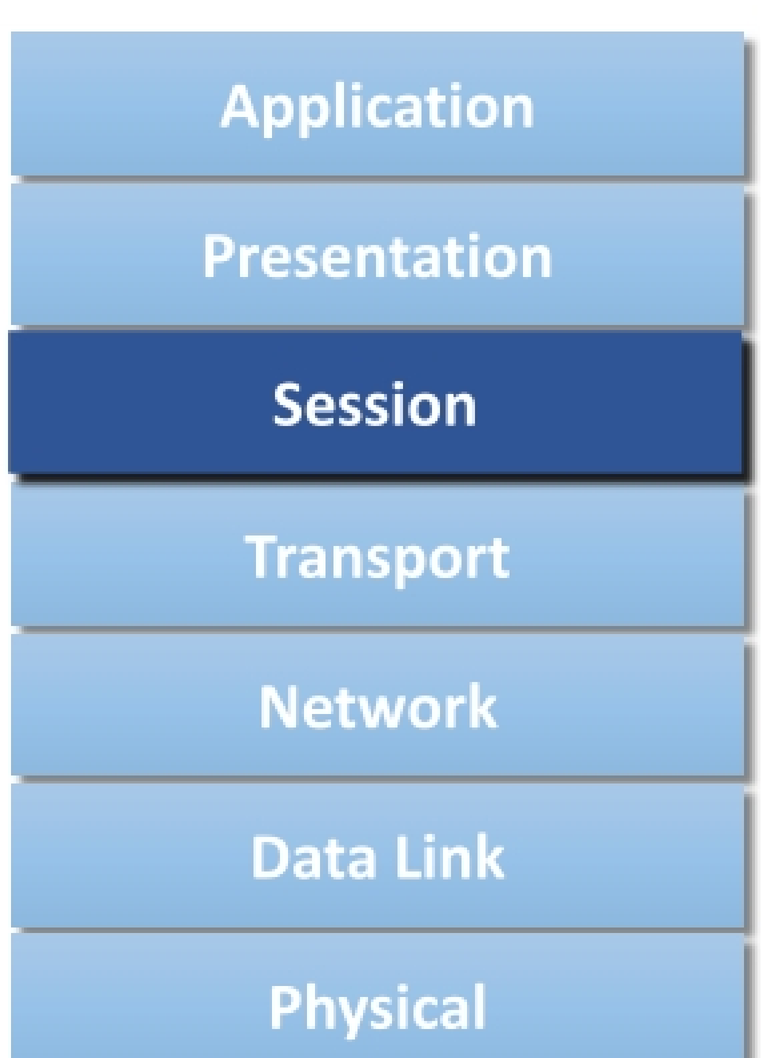
  MPEG,DAT,AVI (Video)

- Encryption – Decryption
- Compression – Decompression

Data flow from Presentation Layer



Session Layer



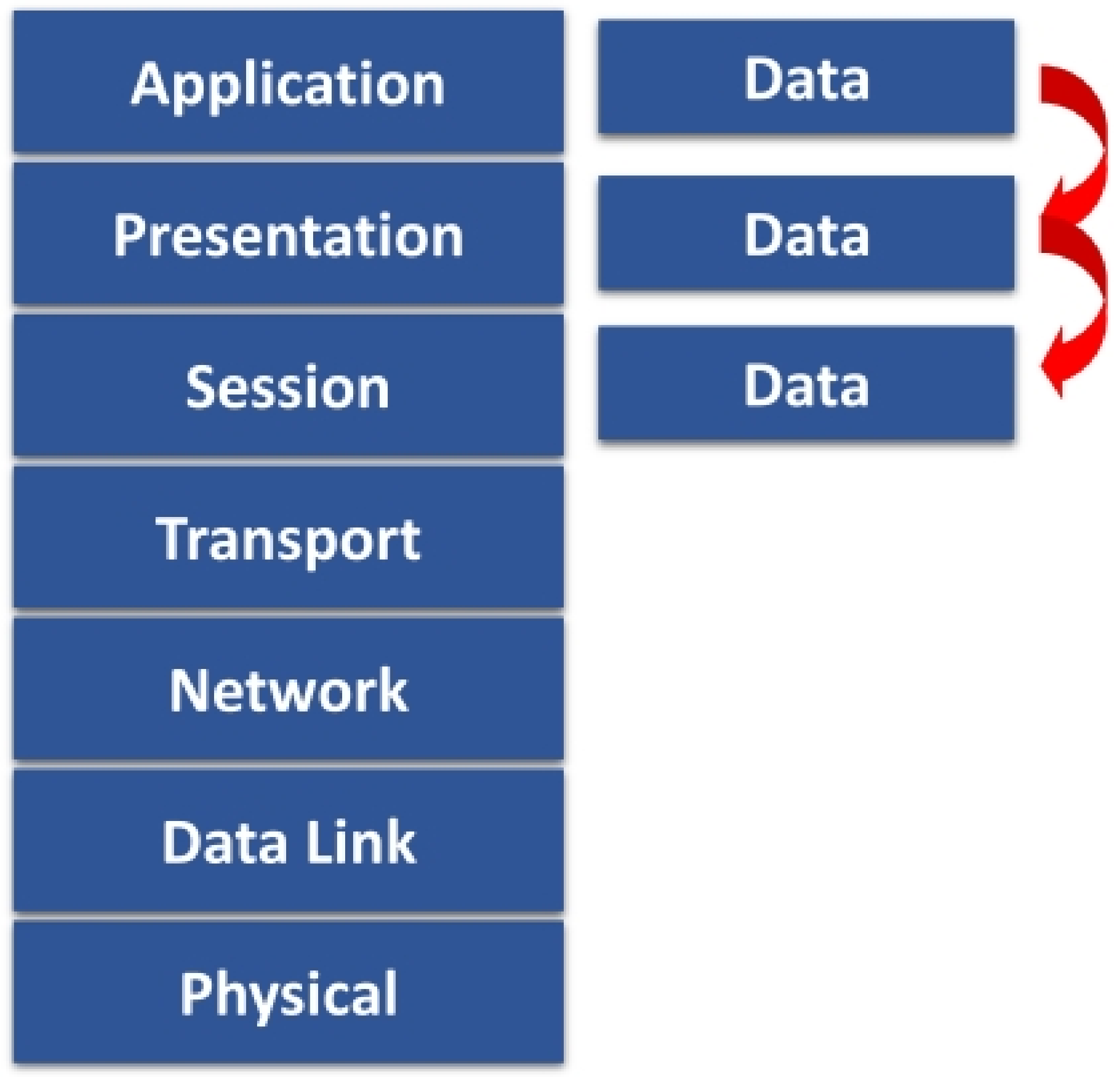
It is responsible for establishing, maintaining and terminating the sessions.

Session ID is used to identify a session or interaction.

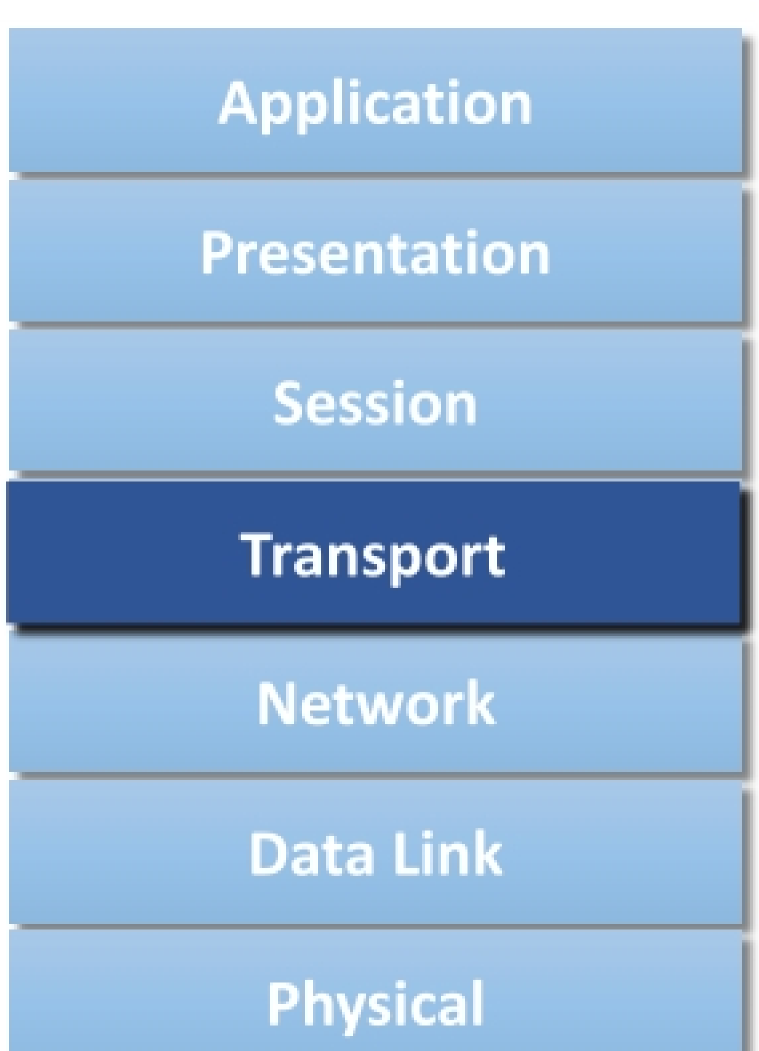
Ex :

- **RPC Remote Procedural Call**
- **SQL Structured Query Language**
- **ASP AppleTalk Session protocol**

Data flow from Session Layer



Transport Layer



It provides data delivery mechanism between the applications in the network.

The major functions described at the Transport Layer are.

- Identifying Service
- Multiplexing & De-multiplexing
- Segmentation
- Sequencing & Reassembling
- Error Correction
- Flow Control

Identifying a Service

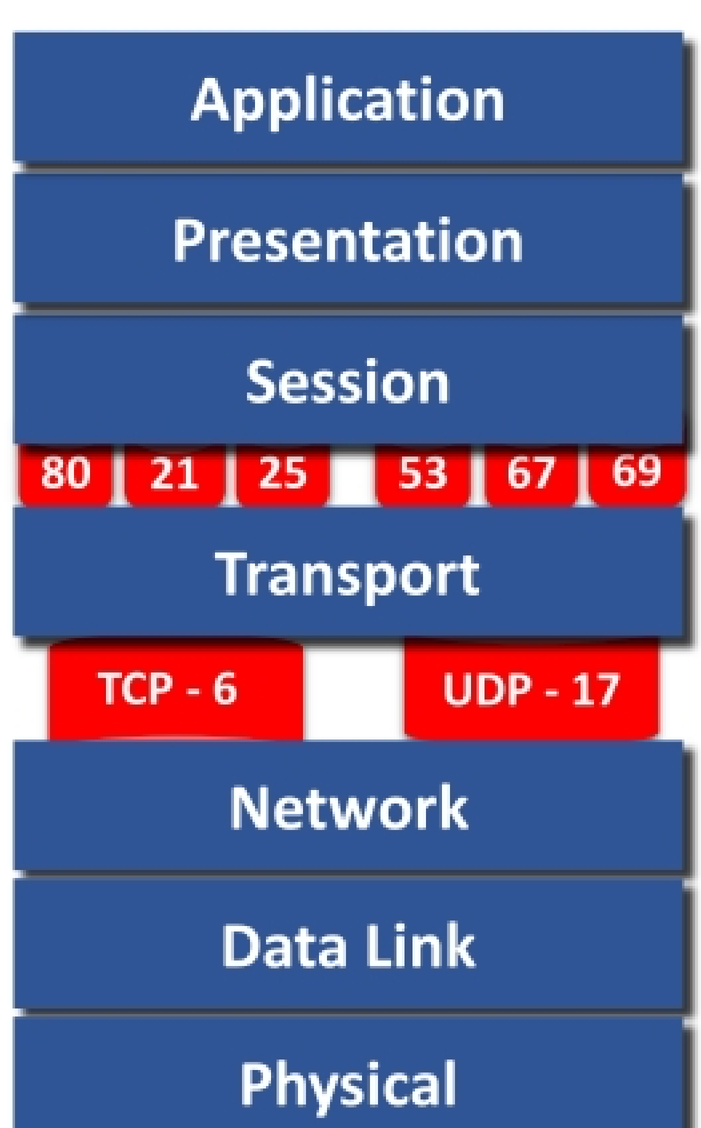
- Identification of Services is done using port Numbers.
- Port is a logical communication Channel

Total No. Ports	0 – 65535
Reserved Ports	1 - 49151
Open Ports	49152 – 65535

Command to check the ports used by the PC (Windows / Linux)

netstat

Multiplexing & De-multiplexing

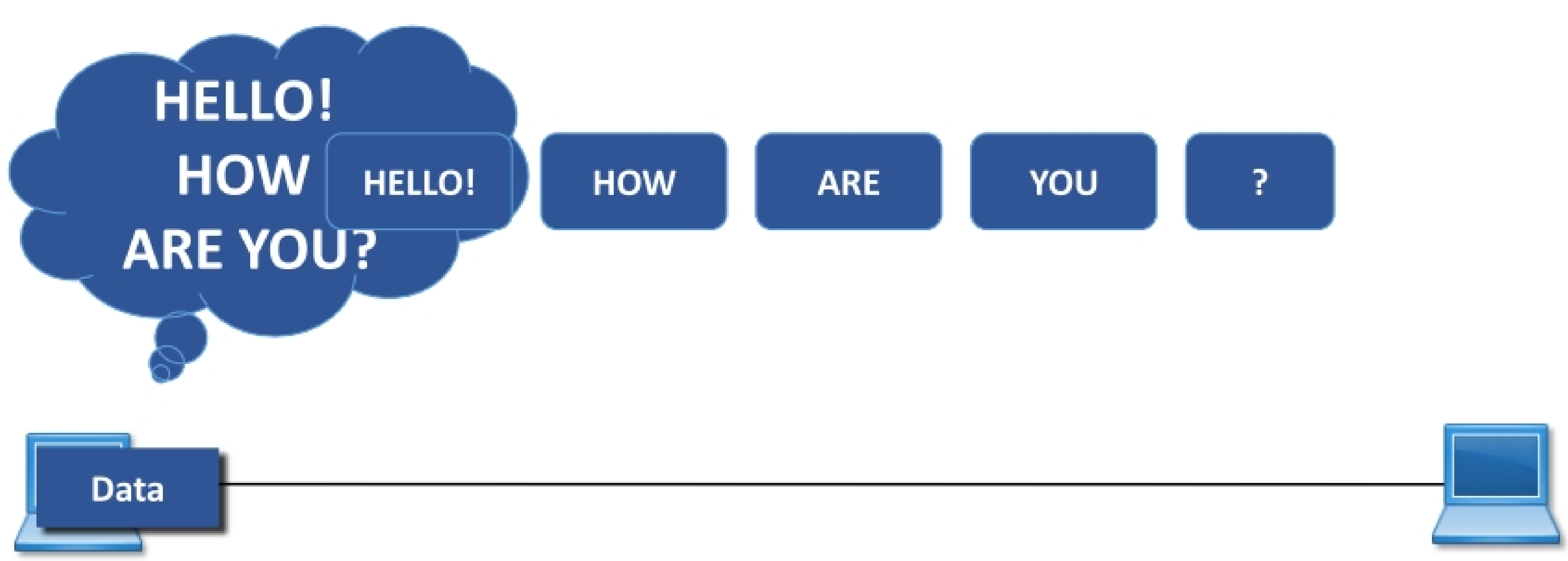


Transport Layer Protocols

- **The protocols which takes care of Data Transportation at Transport layer are TCP and UDP**

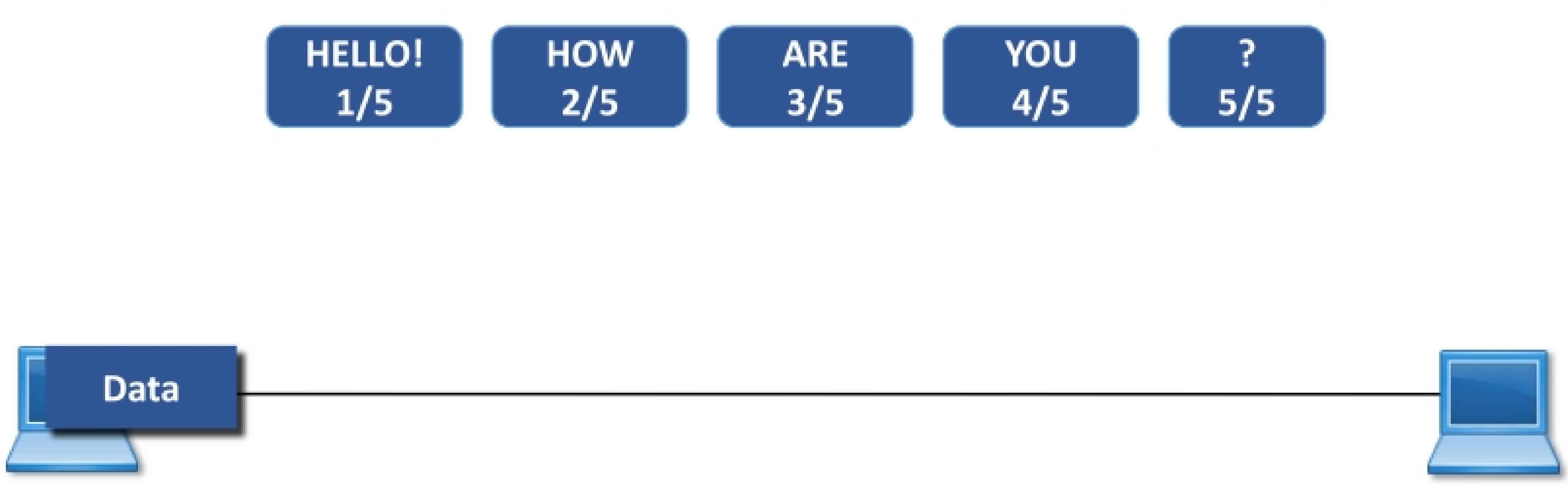
TCP	UDP
Transmission Control Protocol	User Datagram Protocol
Connection Oriented	Connection Less
Supports Acknowledgements	No support for Acknowledgements
Reliable communication	Unreliable communication
Slower data Transportation	Faster data Transportation
Protocol No is 6	Protocol No is 17
Ex: HTTP, FTP, SMTP	Ex: DNS, DHCP, TFTP

Segmentation

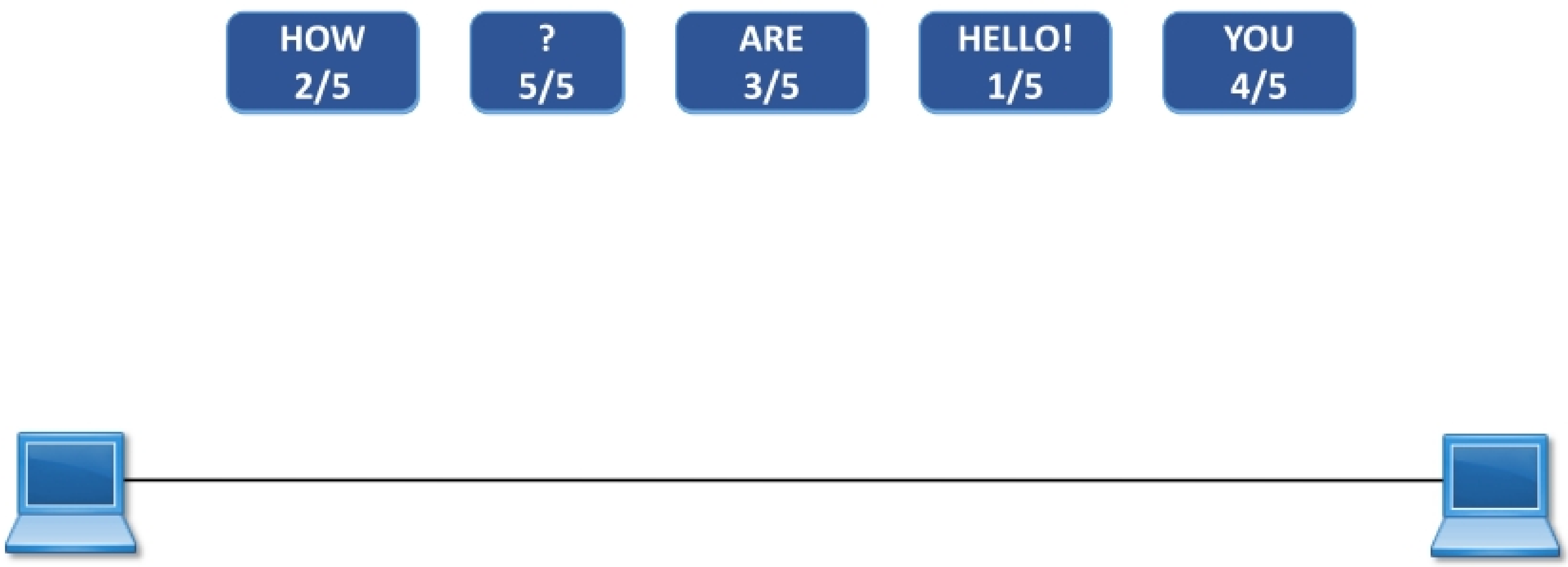


Sequencing

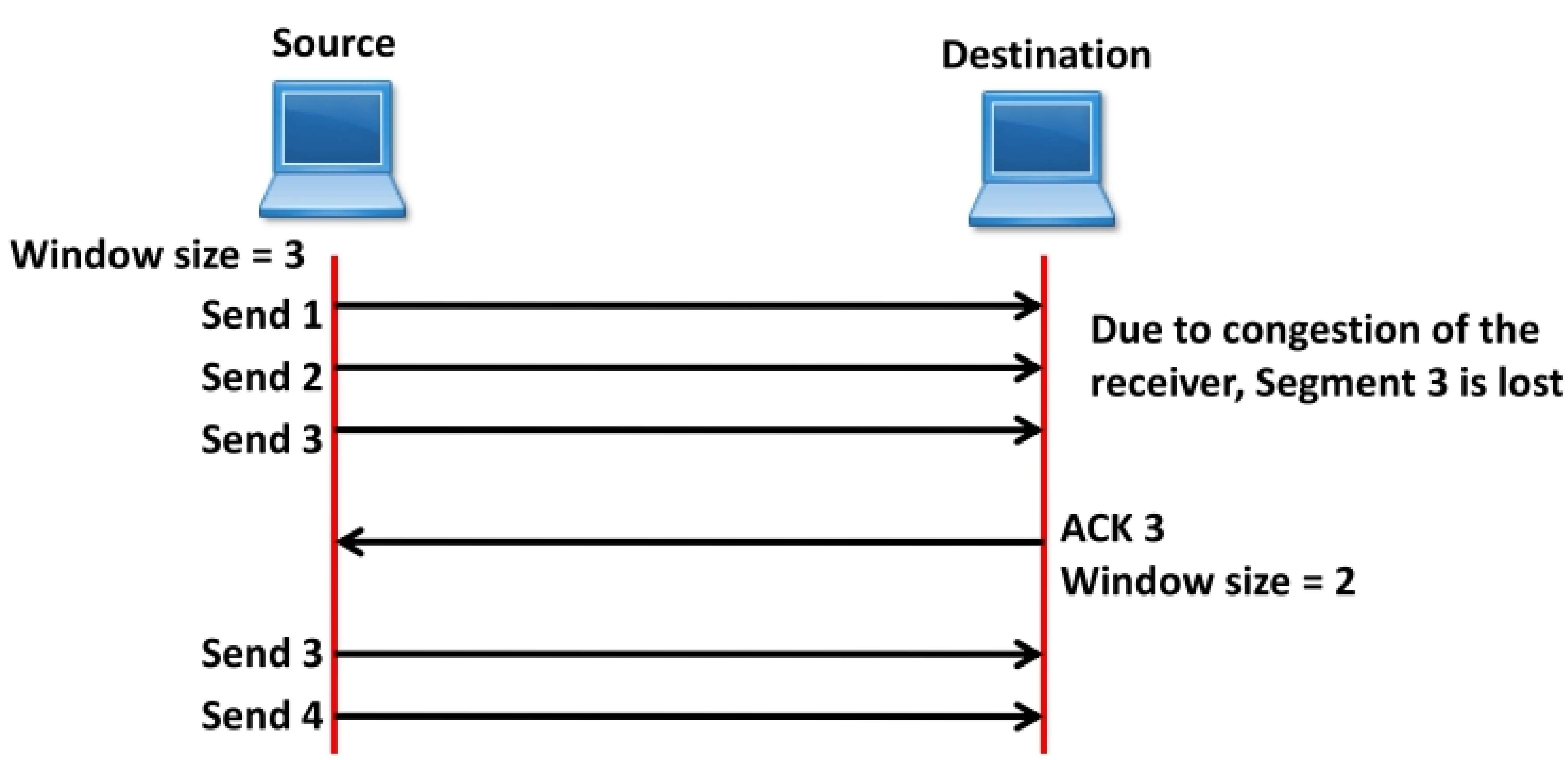
Sequencing



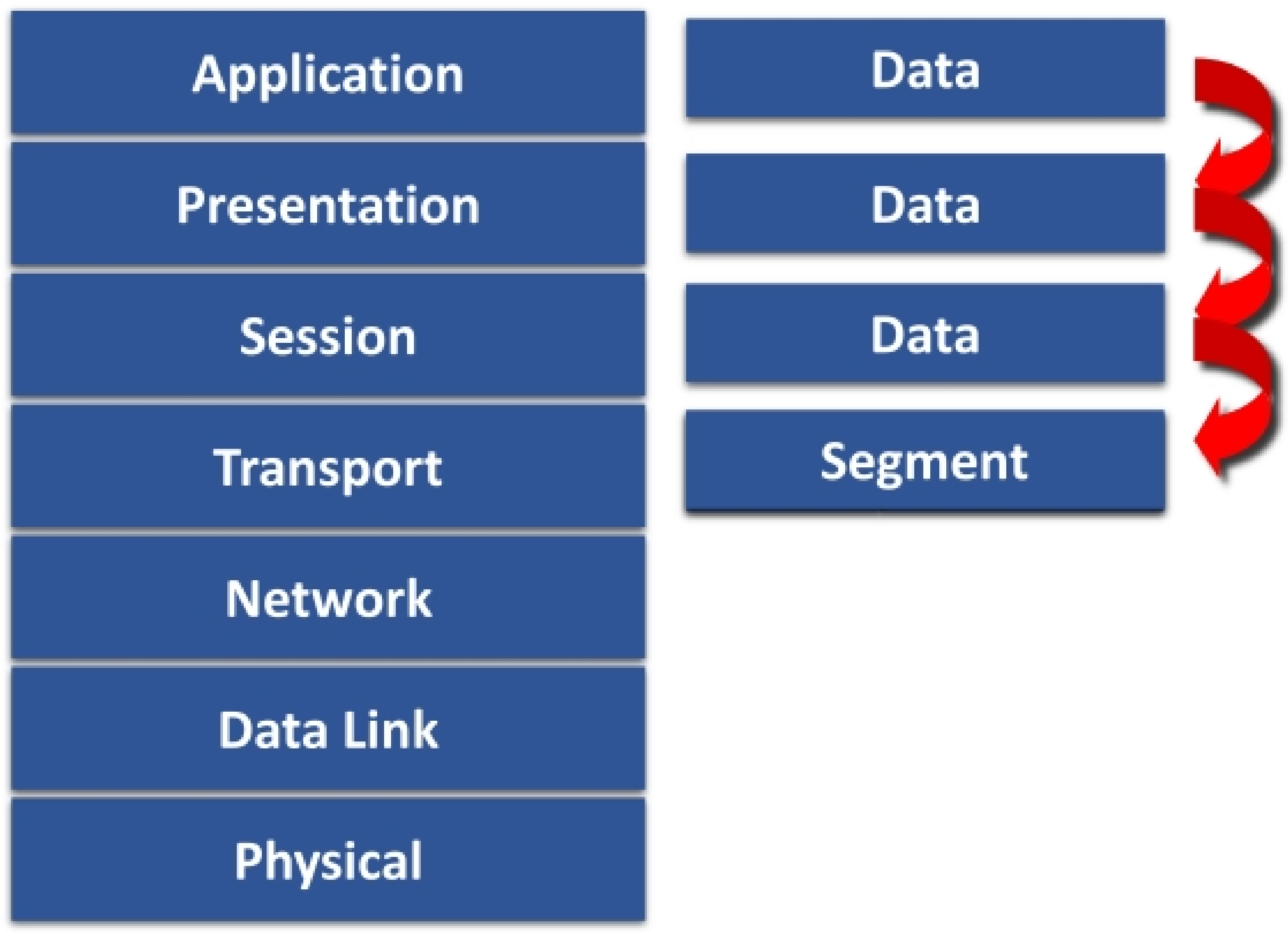
Reassembling



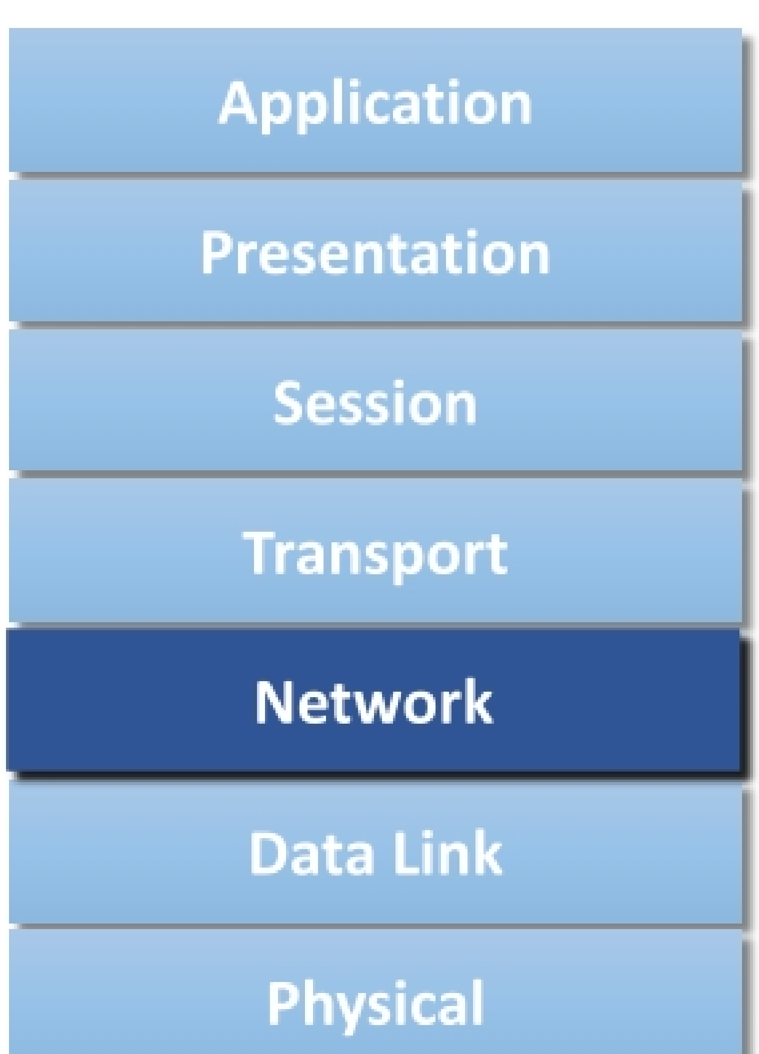
Flow Control and Error Correction



Data flow from Transport Layer



Network Layer



It provides Logical addressing & Path determination (Routing)

The protocols that work in this layer are:

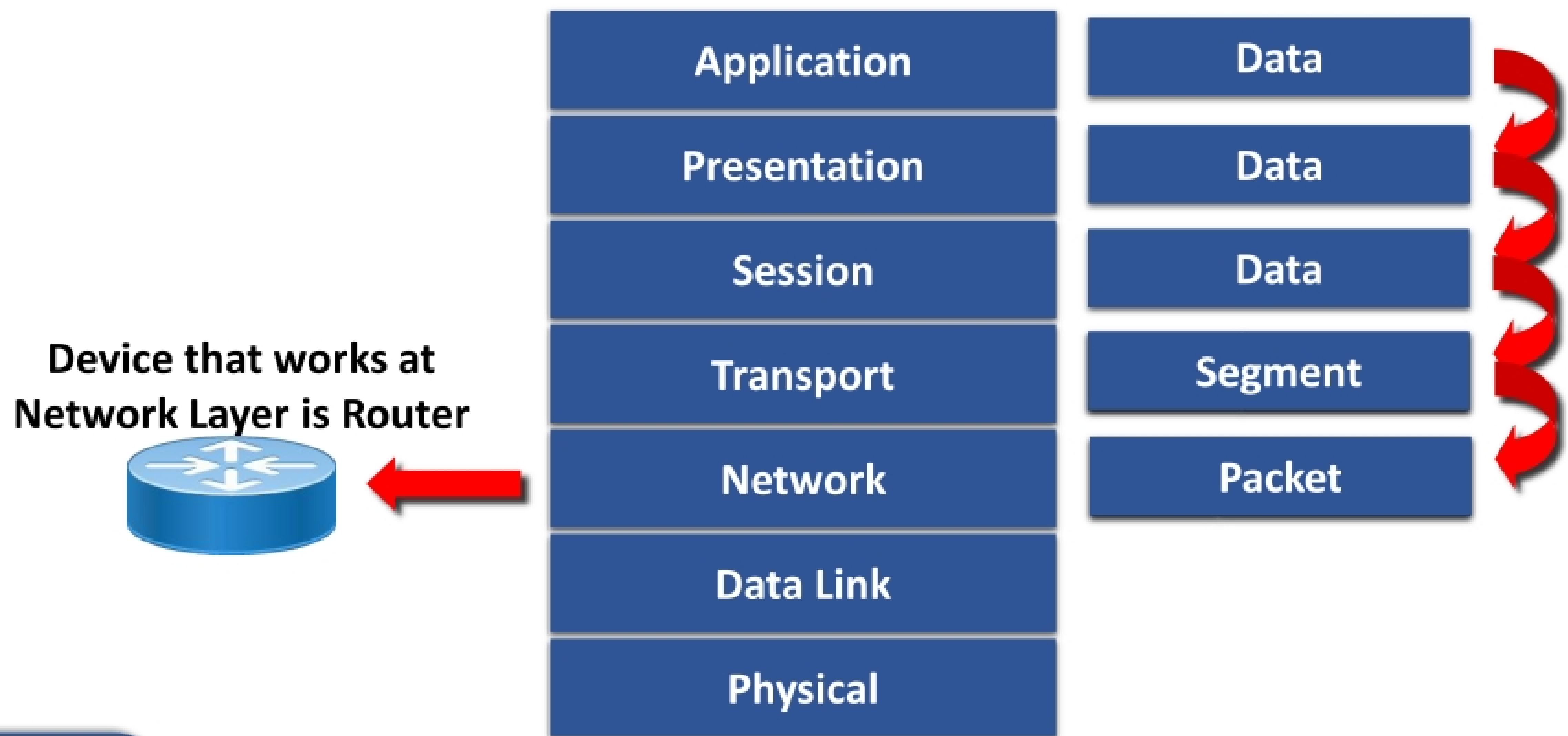
Routed Protocols :

- IP, IPX, AppleTalk.. Etc
- Routed protocols used to carry user data between hosts.

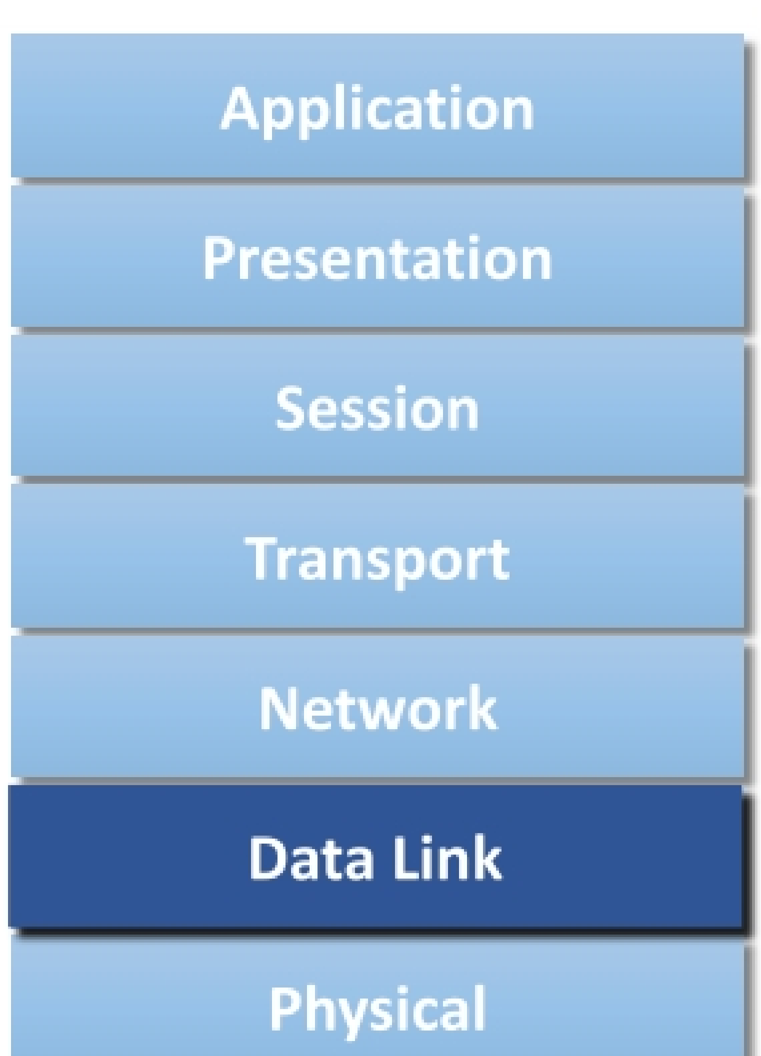
Routing Protocols :

- RIP, OSPF.. Etc
- Routing protocols performs Path determination (Routing).

Data flow from Network Layer



Datalink Layer



It has 2 sub layers

- MAC (Media Access Control)

  It provides reliable transit of data across a physical link.

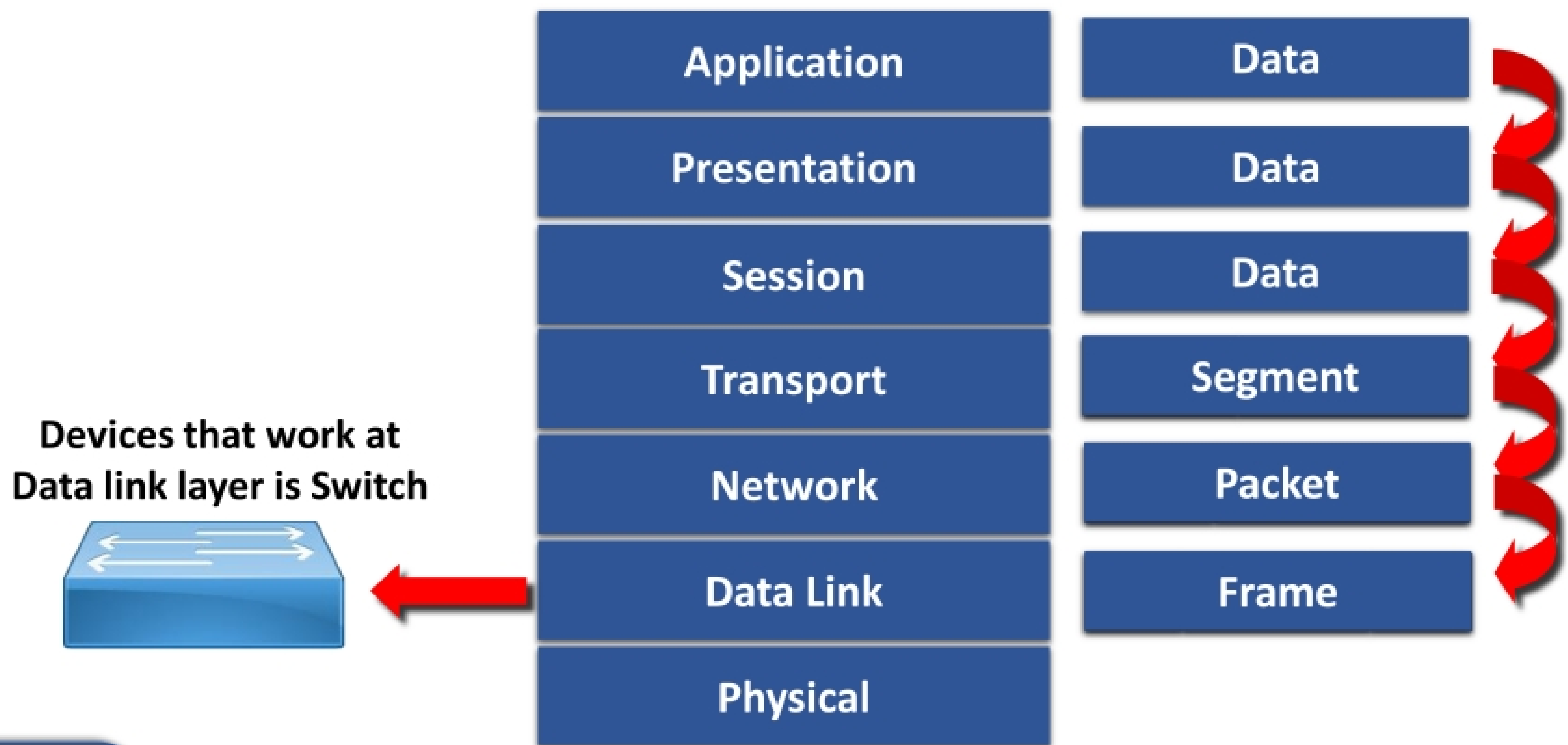
  It also provides ERROR DETECTION using CRC (Cyclic Redundancy Check)

  Ex: Ethernet, Token ring…etc

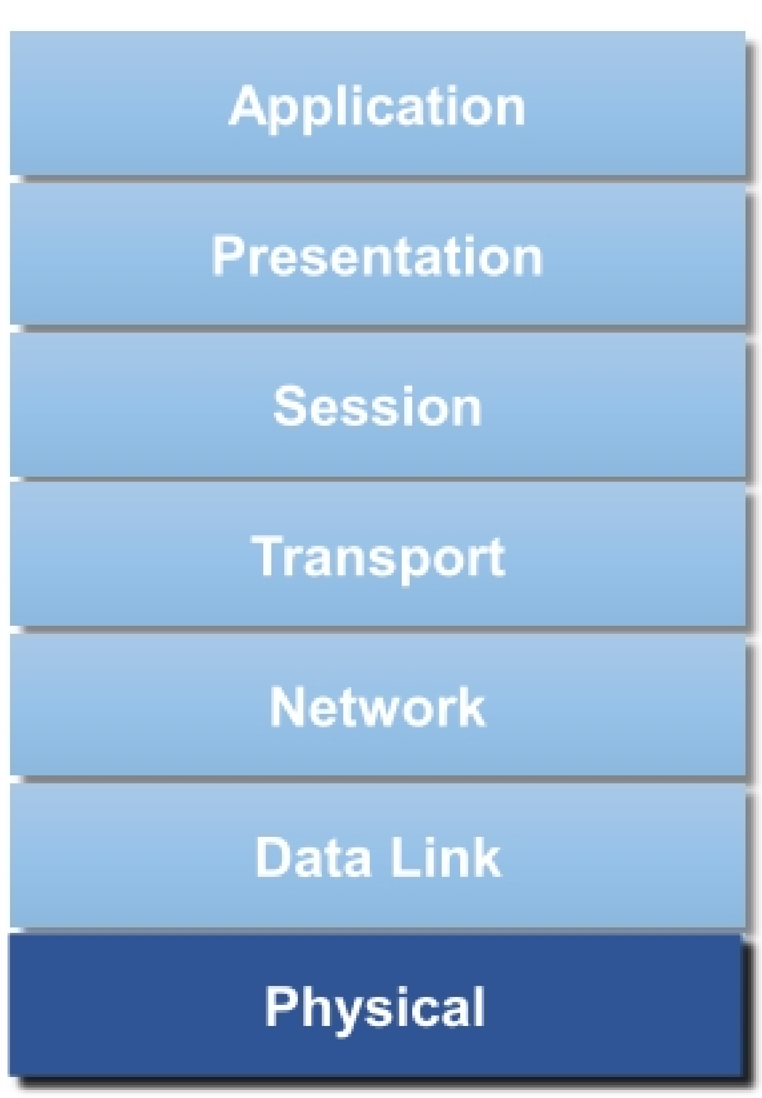
- LLC (Logical Link Control)

  It provides communication with Network layer.

Data flow from Data link Layer



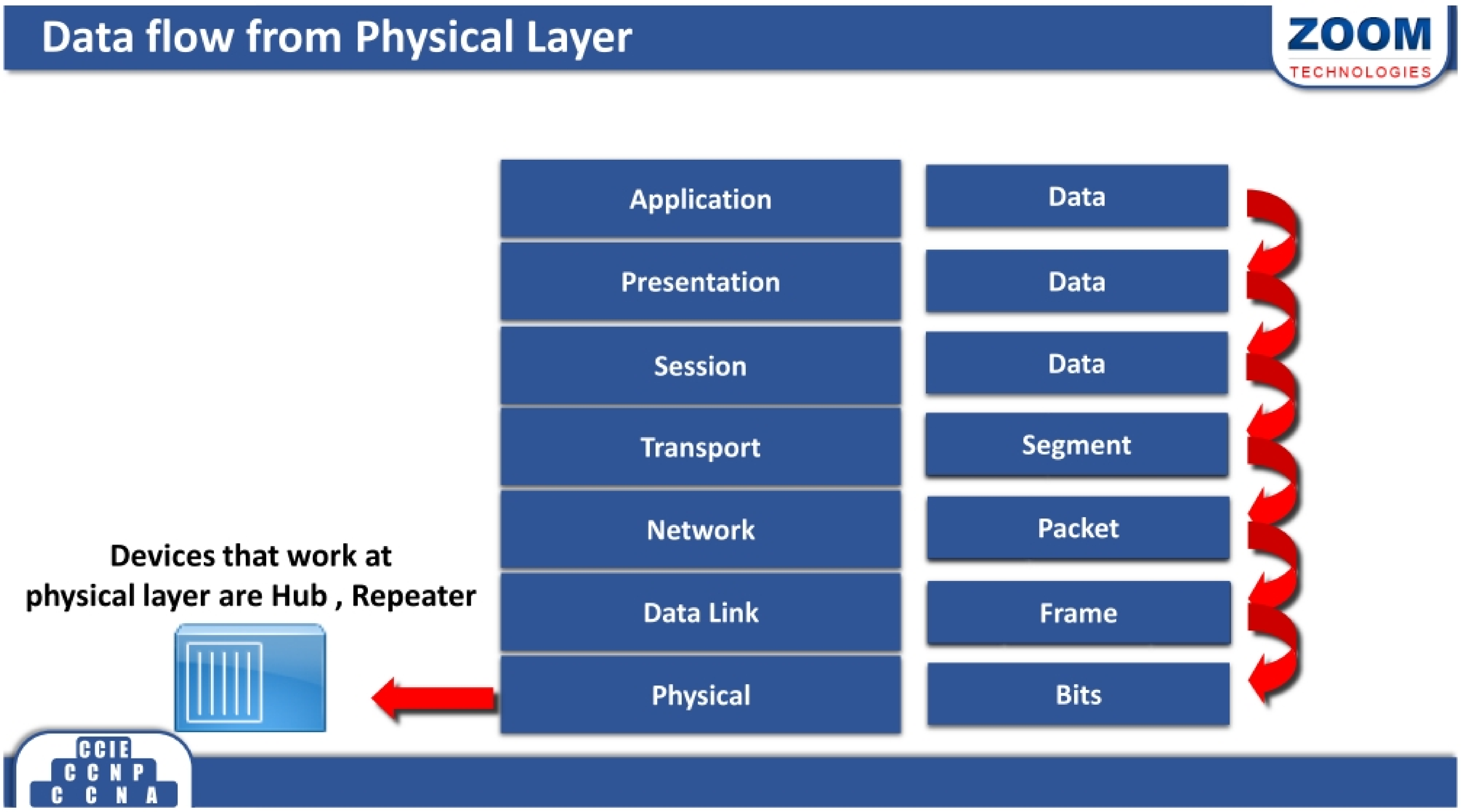
Physical Layer

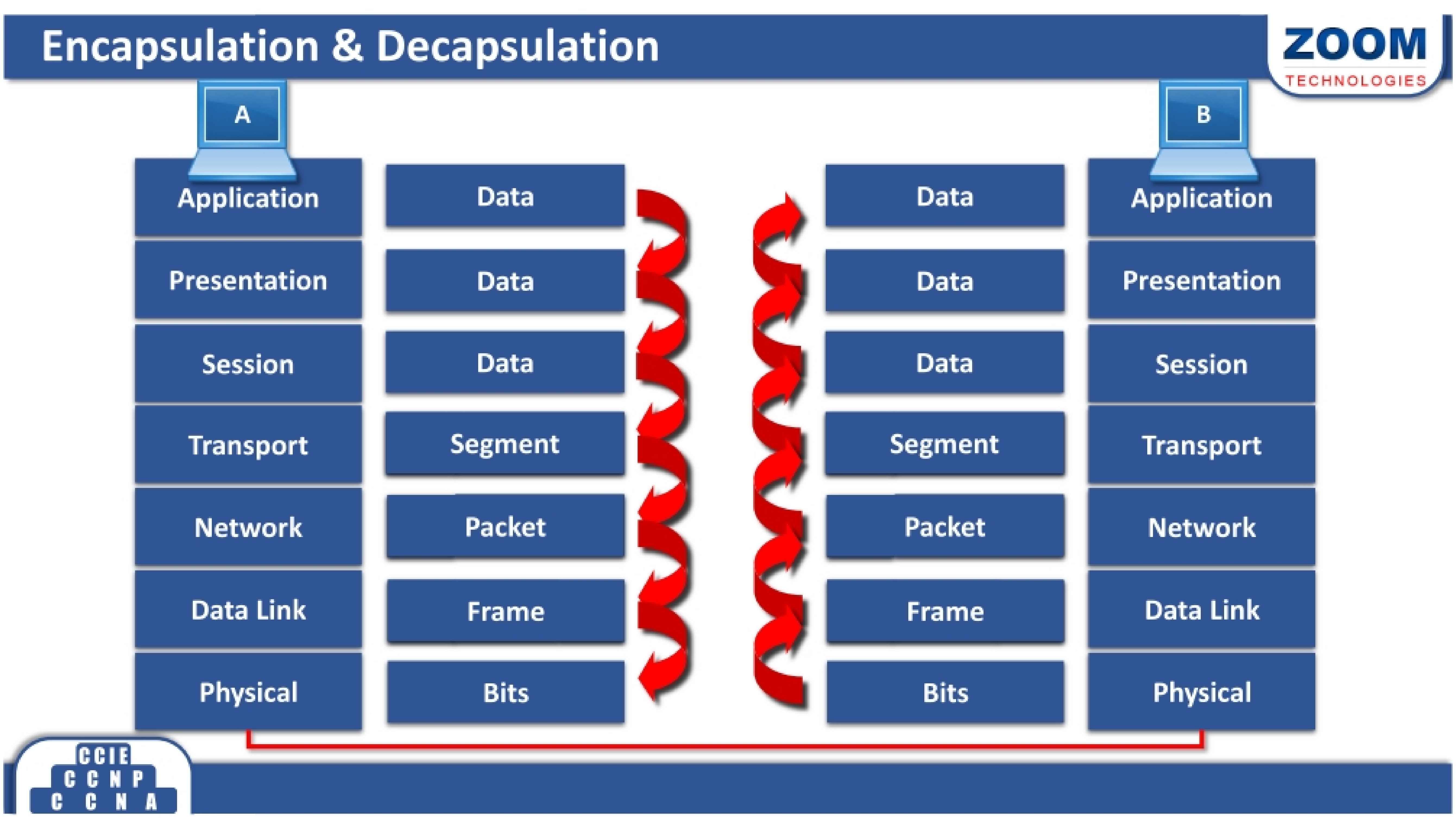


- It defines the electrical, Mechanical & functional specifications for communication between the Network devices.
- The functions described at this layer are
  - Encoding/decoding:

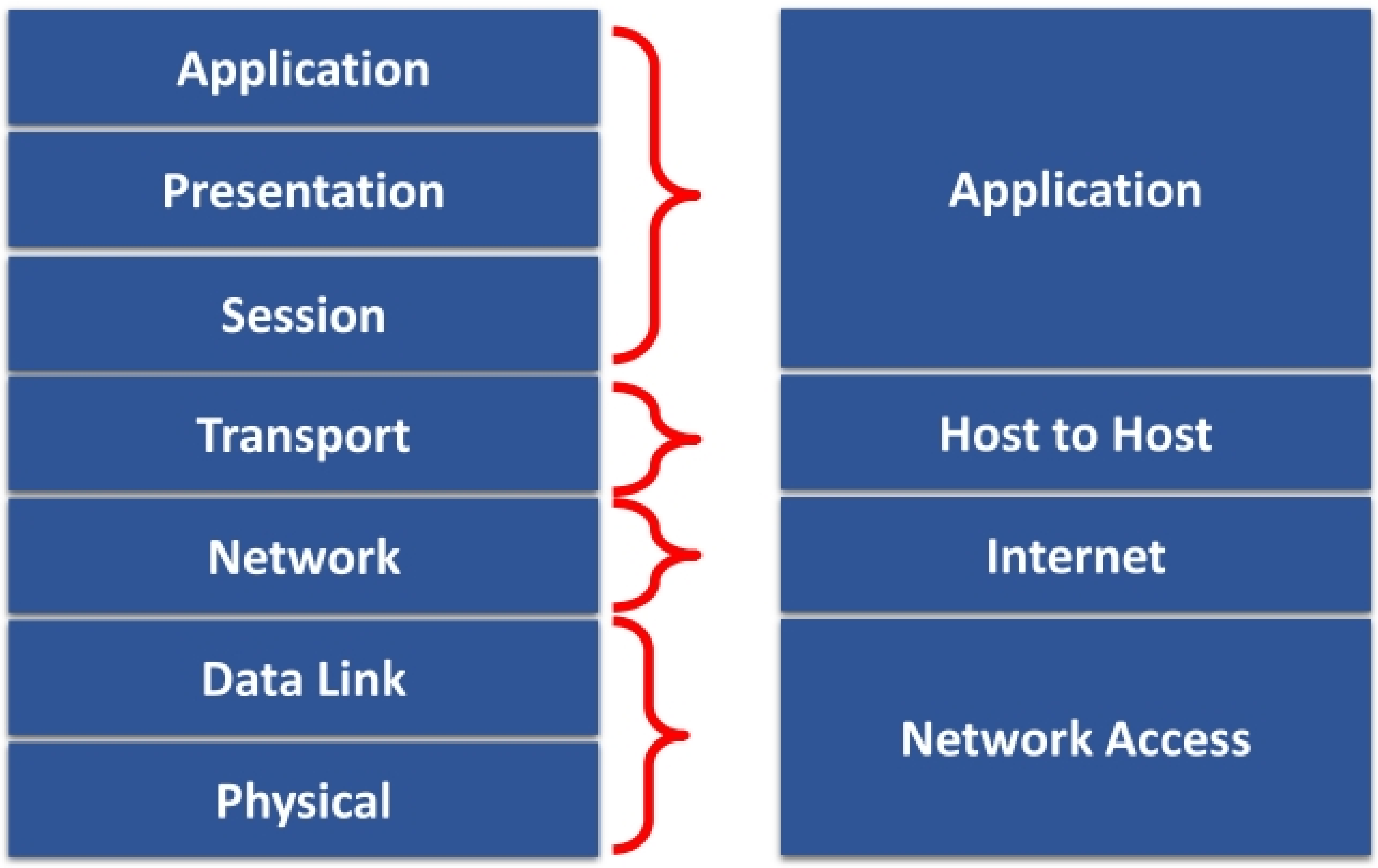
It is the process of converting the binary data into signals based on the type of the media.

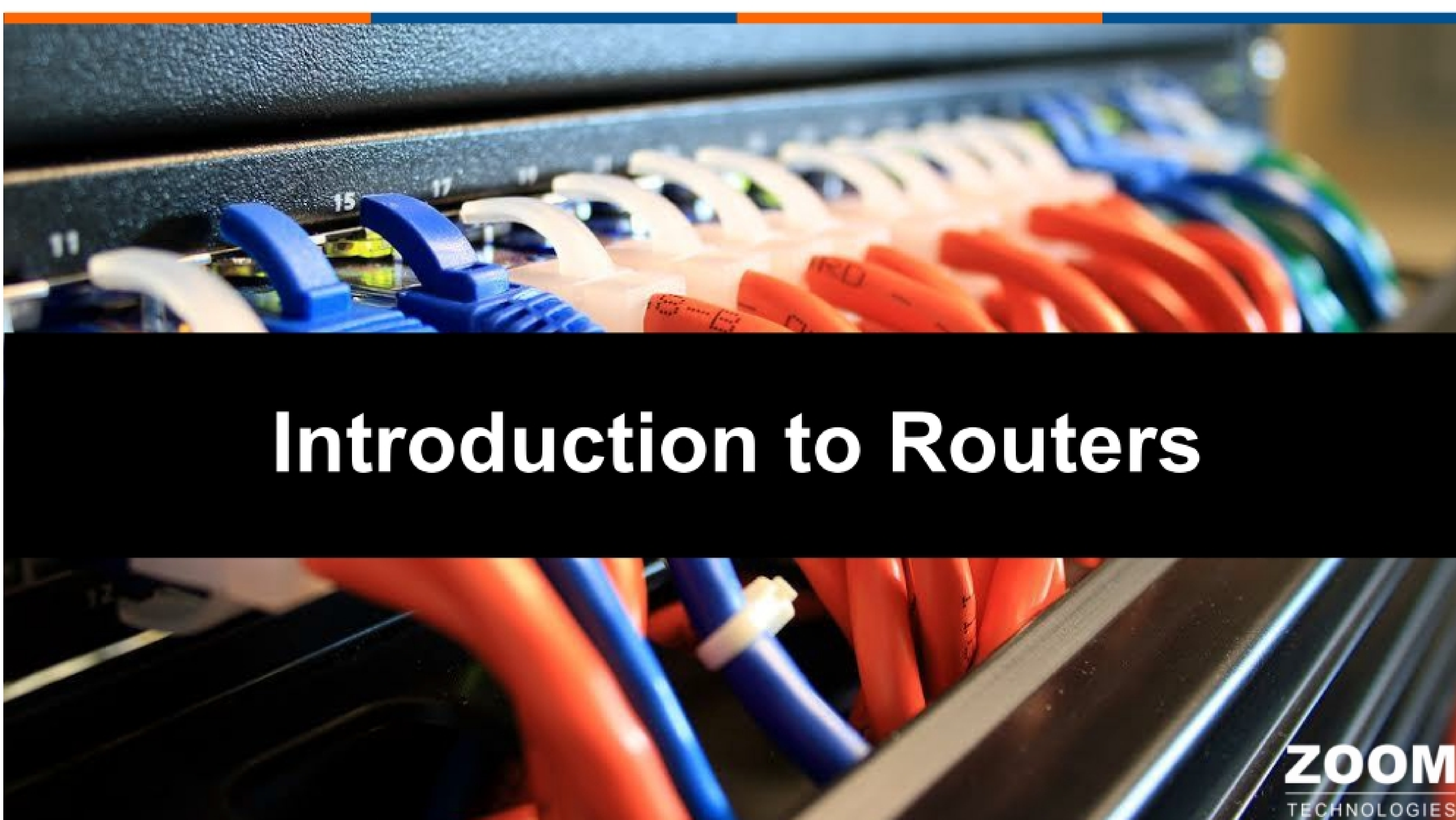
- Copper media : Electrical signals of different voltages
- Fiber media: Light pulses of different wavelengths
- Wireless media: Radio frequency waves


Data flow from Physical Layer
ZOOM
TECHNOLOGIES
Application
Presentation
Session
Transport
Network
Data Link
Physical
Data
Data
Data
Segment
Packet
Frame
Bits
Devices that work at
physical layer are Hub , Repeater
CCIE
CCNP
CCNA


Encapsulation & Decapsulation
ZOOM
TECHNOLOGIES
A
B
Application
Presentation
Session
Transport
Network
Data Link
Physical
Data
Data
Data
Segment
Packet
Frame
Bits
Data
Data
Data
Segment
Packet
Frame
Bits
Application
Presentation
Session
Transport
Network
Data Link
Physical
CCIE
CCNP
CCNA

Comparison between OSI & TCP/IP Model





Router

- Router is an internetworking device.
- It enables communication between two or more different logical networks.
- It is a Network Layer (layer 3) device.
- It comes from the word "ROUTE". Hence it is also a device that finds the best route (path) for networks.
- The IP of Router is the default gateway for all devices in LAN.

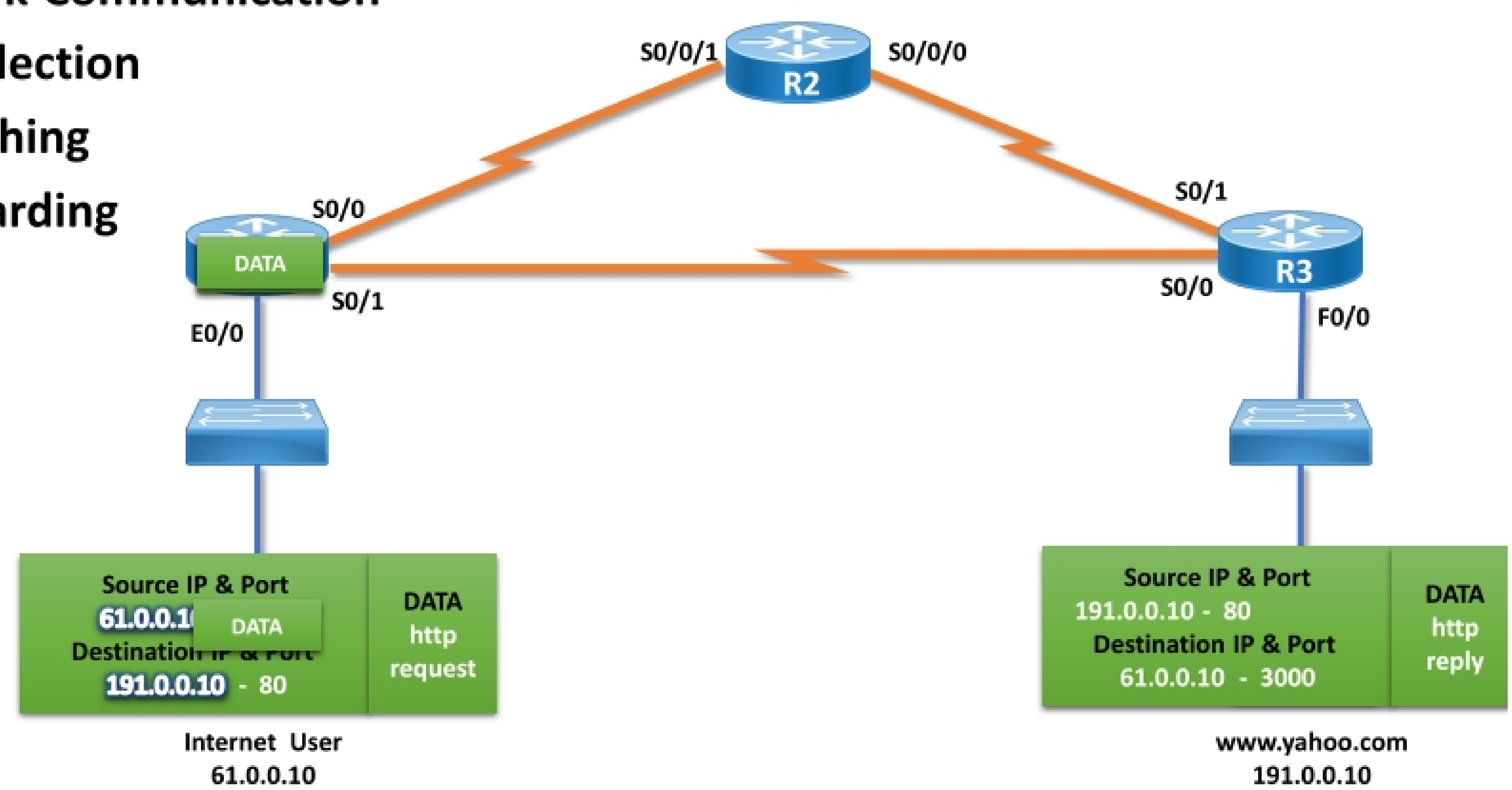
Type of Routers

There are two type of Routers

- Hardware Routers:
  - Cisco, Juniper, Multicom, HP, Dlink, Maipu and many more…
- Software Routers:
  - Microsoft Server, Linux Server

Functions of a Router

- Inter-network Communication
- Best Path Selection
- Packet Switching
- Packet forwarding



Types of Routers

- Fixed router
  - Fixed routers are non upgradable, can not add or remove the Ethernet or serial ports.
  - Does not have any slot.
  - In fixed routers the ports are integrated on the mother board.(Fixed on mother board).
- Modular router
  - Modular Routers are upgradable, can add or remove the interfaces as per our requirement.
  - Number of slots available depends on the series of the router.
  - Can add LAN and WAN cards.

Fixed router and Modular router

Cisco Router Category

- **Branch Routers**
- **Network Edge and Aggregation Routers**
- **Service Provider Routers**

Branch Routers

- Routers used by small organization and branch offices
- Router Series - Models
  - 800 series - 810, 860, 880
  - 1900 series - 1905, 1921, 1941
  - 2600 series - 2610, 2611, 2620
  - 2800 series - 2811, 2851
  - 2900 series - 2901,2911,2921

Network Edge and Aggregation Routers

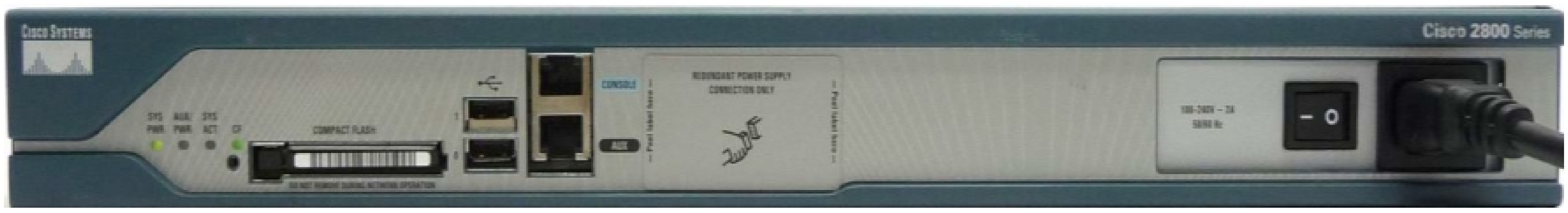
- Routers that are used at large organization / campus and Head Offices
- Router Series - Models
  - 1000 series - 1001, 1002, 1004
  - 5000 series - 5001, 5002
  - 5500 series - 5508

Service Provider Routers

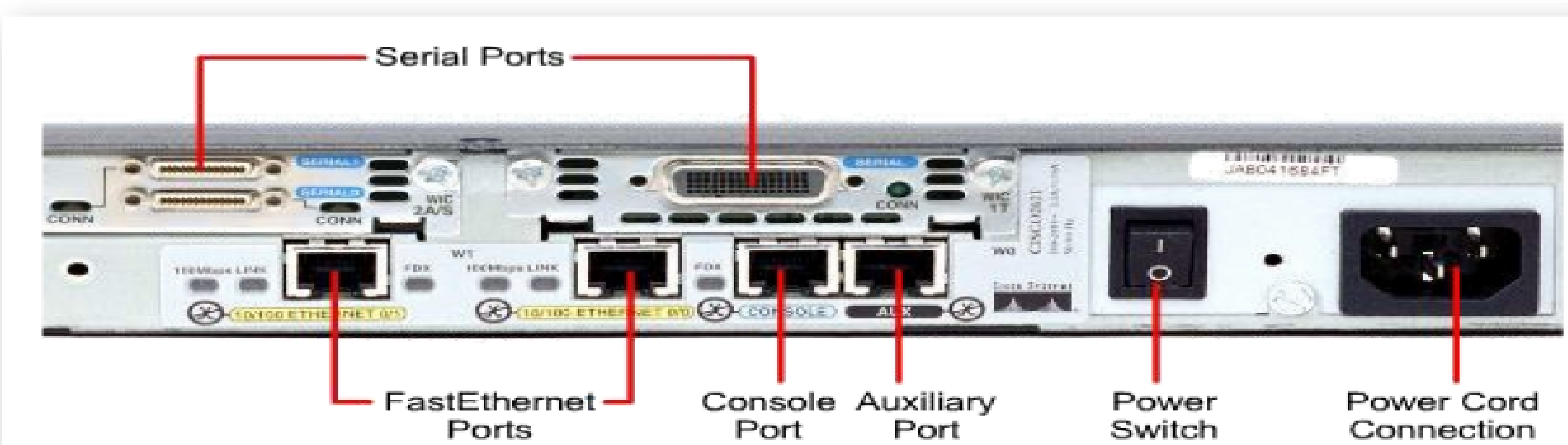
- Routers that are used by the service providers.
- Router Series
  - 6000 series
  - 9000 series

External Components of a Router

2800 Series

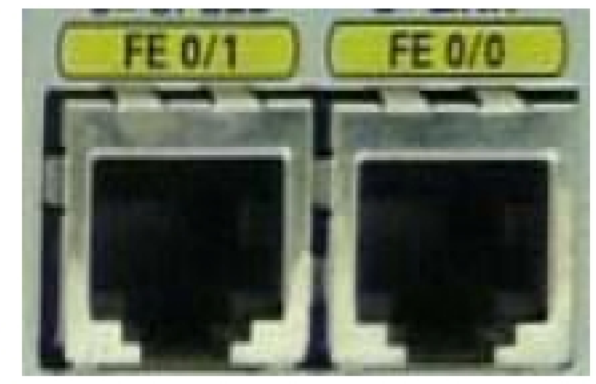


Interfaces on Router



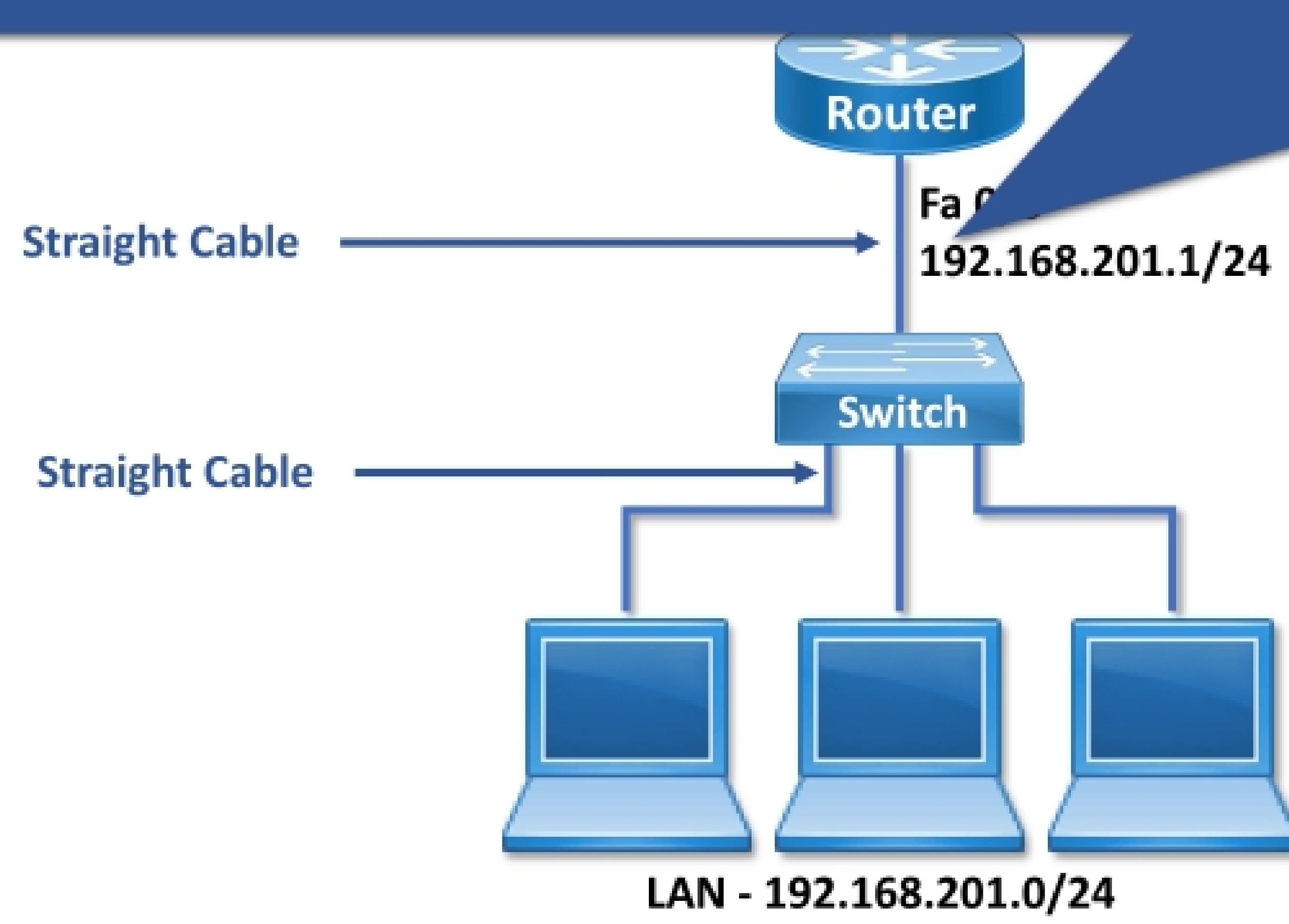
LAN Interfaces - RJ-45 ports

- Routers have RJ-45 ports to connect the Router to the LAN.
- The speed of the RJ-45 ports can be
  - 10 Mbps Ethernet
  - 10/100 Mbps Fast Ethernet
  - 10/100/1000 Mbps Gigabit Ethernet

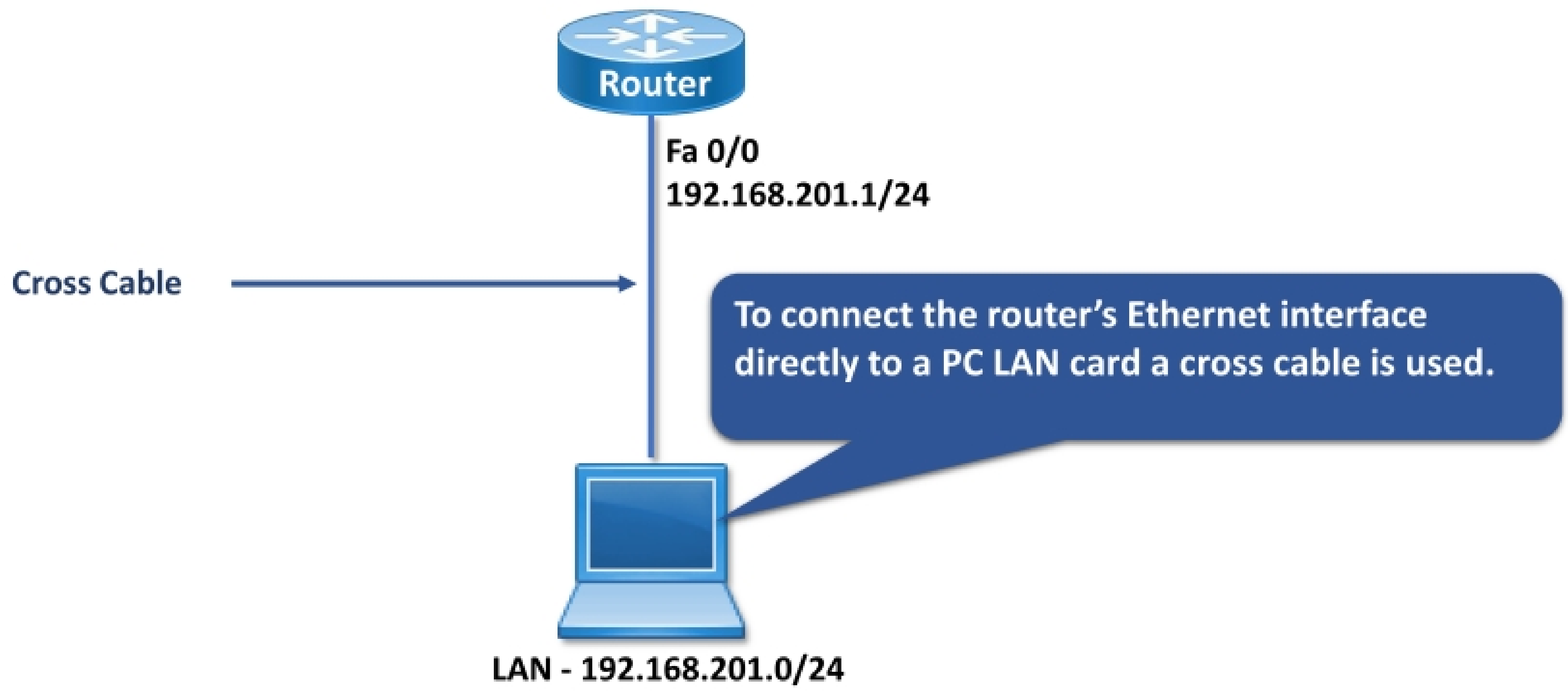


LAN Connectivity

An IP address has to be assigned to this interface. It should be in the same network as that of the LAN. This IP address is the default gateway address for all LAN systems.

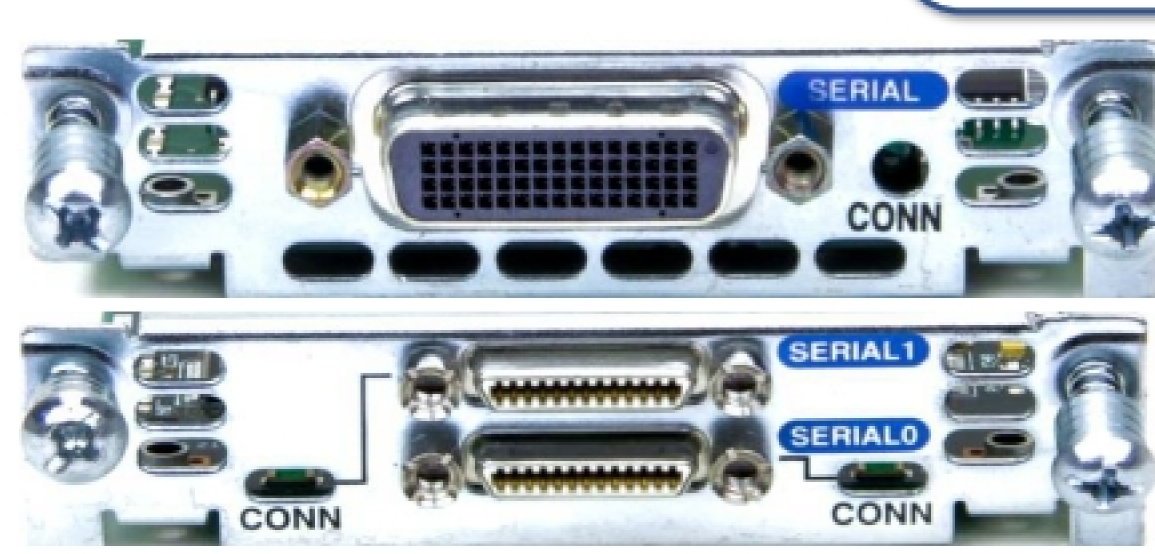


LAN Connectivity



Serial Port

- Serial port is used for WAN Connectivity.
- Serial port are available as
  - 60 pin female connectors.
  - Smart Serial 26 pin female connectors.



HWIC

- High-speed WAN interface cards (HWICs) provide connectivity to a Wide Area Network

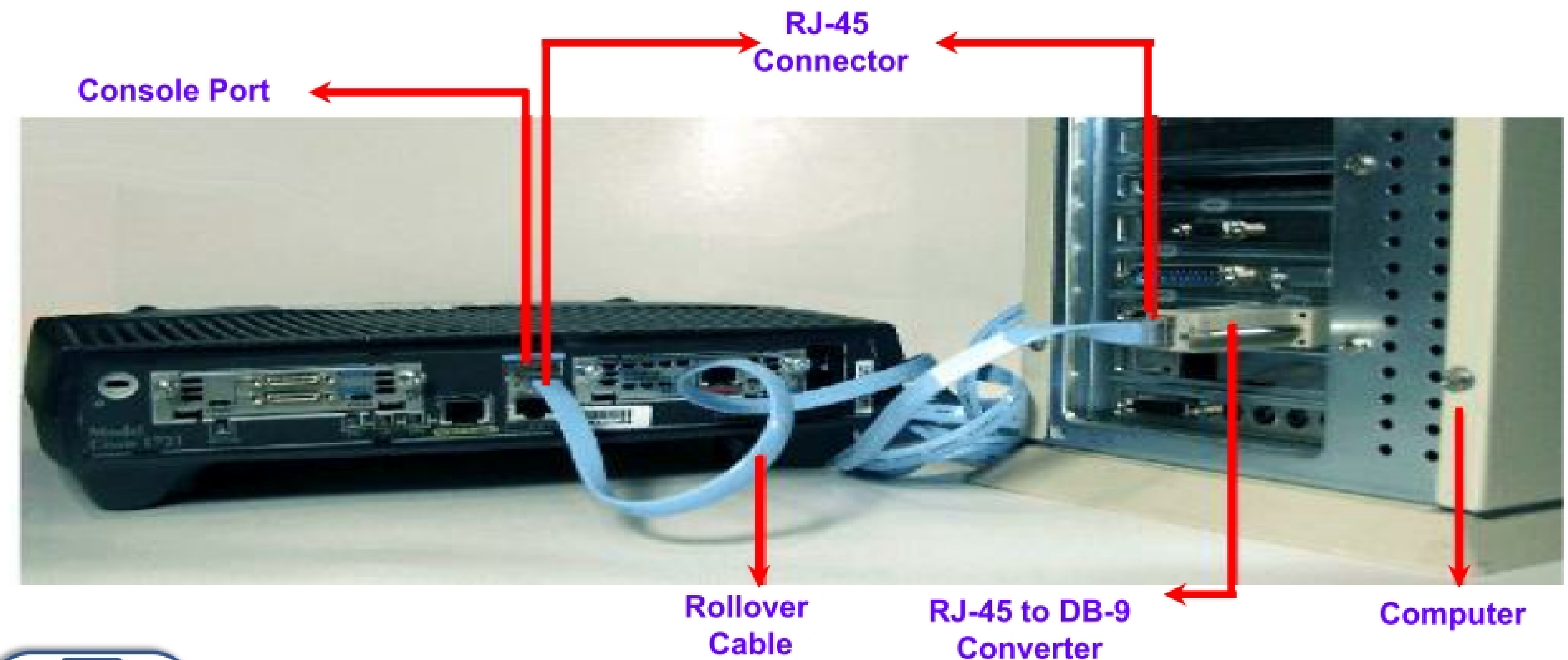
Console Port

- It is a local administrative port.
- It is a RJ-45 Port.
- It is used for initial configuration and advance troubleshooting.
- Note : It is the most important and sensitive port on the Router.

DB-9 Convertor

Console cable

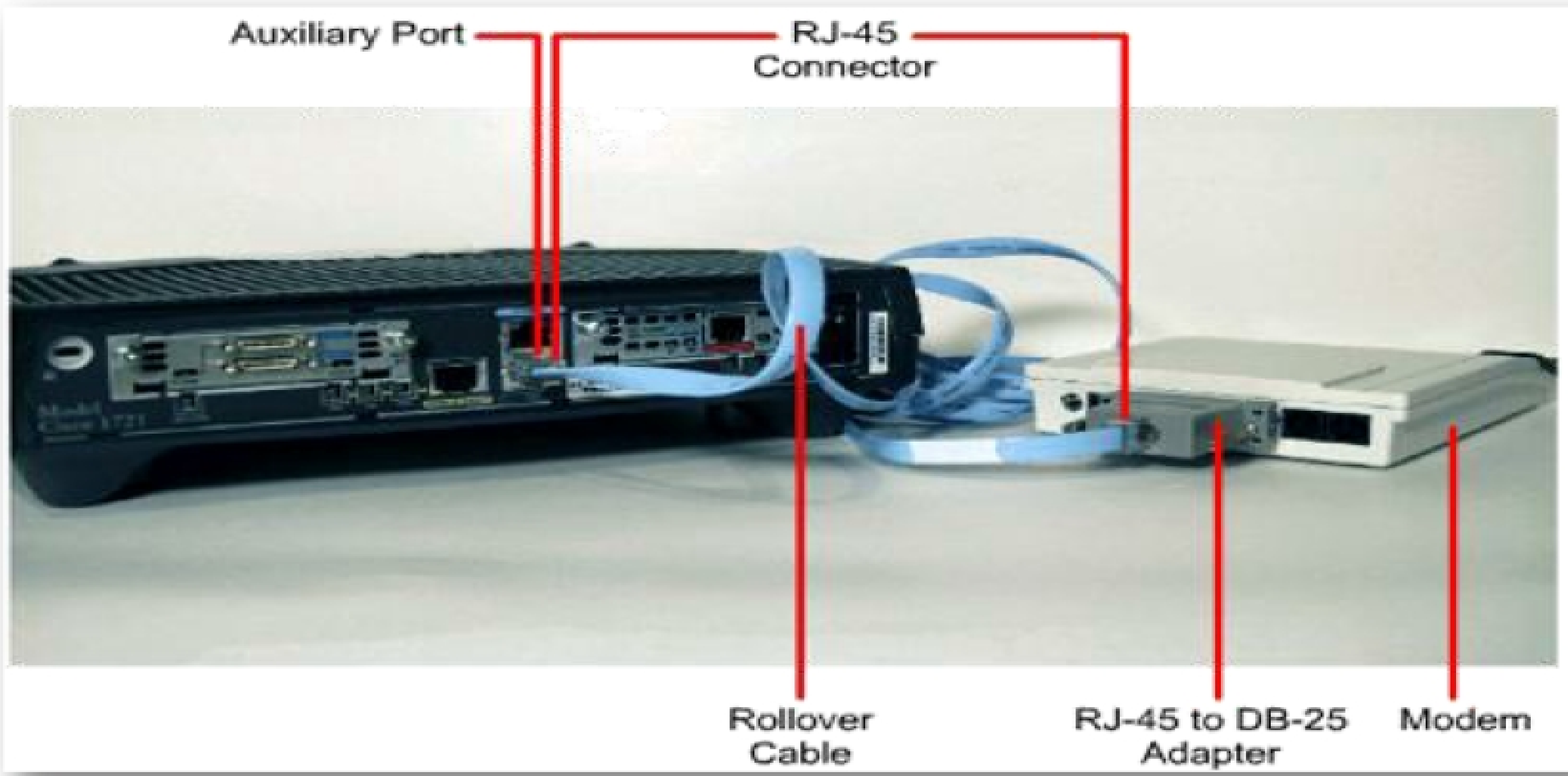
Console Connectivity



Auxiliary Port

- It is a remote administrative port.
- Used for remote administration / configuration.
- Its an RJ-45 port.
- A console / rollover cable is used to connect the auxiliary port to a dial-up modem.

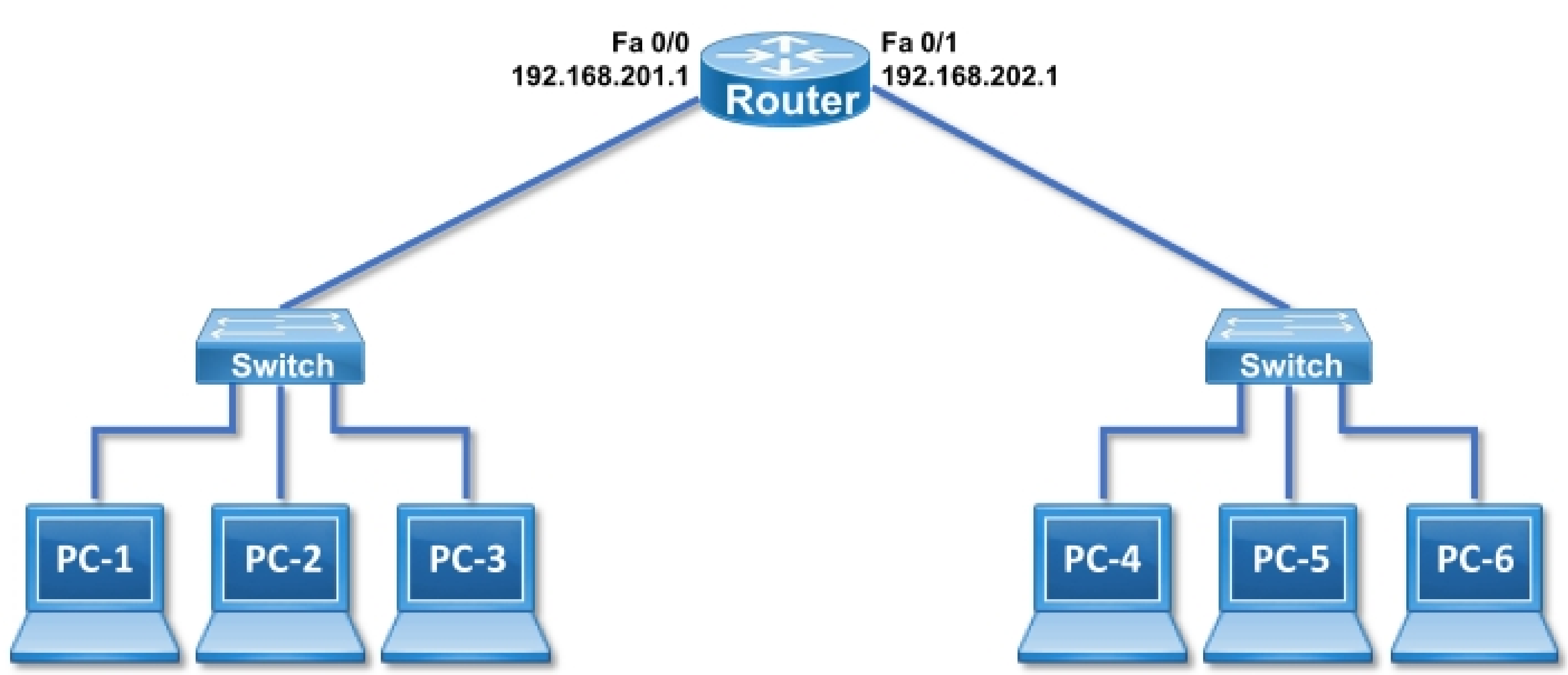
Auxiliary Connectivity



Interfaces of a Router

- LAN Interface
  - RJ 45 Ethernet / FastEthernet / GigabitEthernet
- WAN Interface
  - Normal Serial Interface
  - Smart Serial Interface
- Administrative Interface
  - Console
  - Auxiliary

IPv4 Different Network Communication



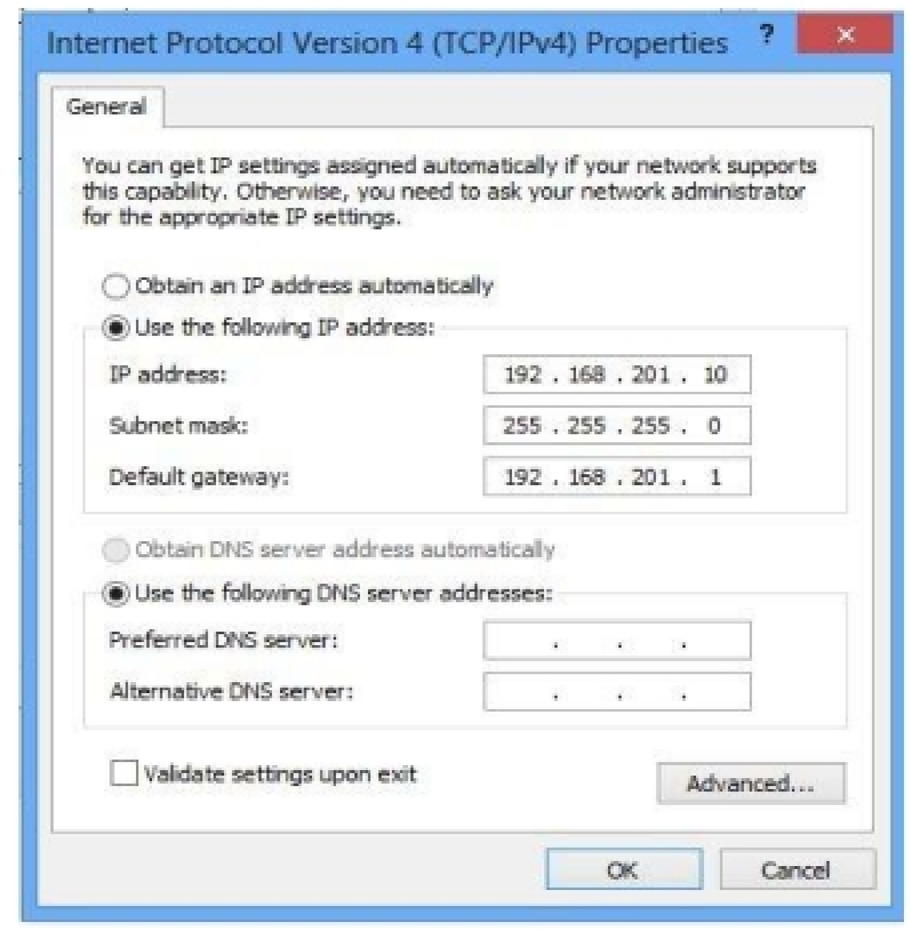
Computer	IP Address / Mask
PC-1	192.168.201.10/24
PC-2	192.168.201.20/24
PC-3	192.168.201.30/24

Computer	IP Address / Mask
PC-4	192.168.202.10/24
PC-5	192.168.202.20/24
PC-6	192.168.202.30/24

Assigning Default Gateway IP Address on Windows Computer

On Windows 7 or Windows 8.x or Windows 10 Computer

- Open **Network and Sharing Center**
- Click on **Change adapter settings** and Click **Open**.
- Right-click on your local adapter and select **Properties**.
- In the Local Area Connection Properties window select **Internet Protocol Version 4 (TCP/IPv4)** then click the **Properties** button.
- Enter **Default Gateway** and click **OK**.



Verify IPv4 Address on Windows Computer

C:\> **ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . : **192.168.201.10**

Subnet Mask . . . . : **255.255.255.0**

Default Gateway . . . . : **192.168.201.1**

C:\>

Assigning Default Gateway IP Address on Linux Computer

bt ~ # **route add default gw 192.168.201.1**

Verify IPv4 Address on Linux Computer

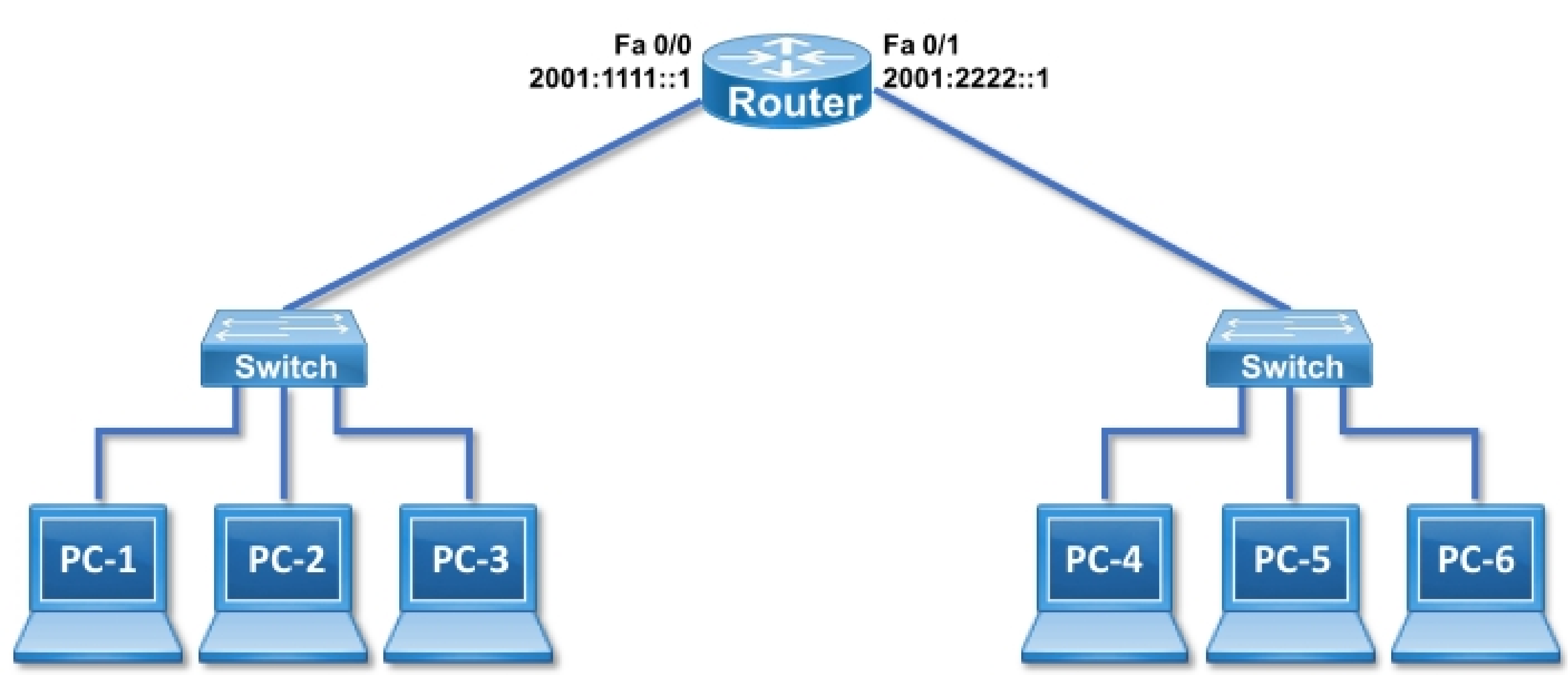
bt ~ # **route -n**

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.201.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	**192.168.201.1**	**0.0.0.0**	**UG**	**0**	**0**	**0**	**eth0**

bt ~ #

IPv6 Different Network Communication



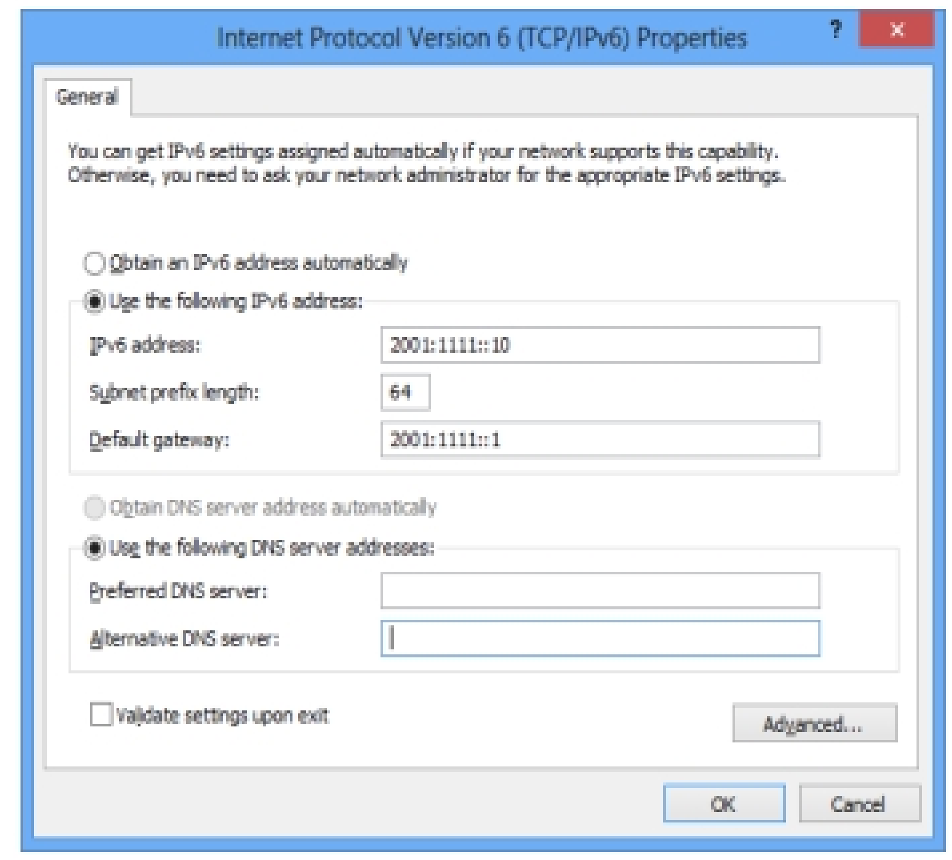
Computer	IP Address / Mask
PC-1	2001:1111::10/64
PC-2	2001:1111::20/64
PC-3	2001:1111::30/64

Computer	IP Address / Mask
PC-4	2001:2222::10/64
PC-5	2001:2222::20/64
PC-6	2001:2222::30/64

Assigning Default Gateway IP Address on Windows Computer

On Windows 7 or Windows 8.x or Windows 10 Computer

- Open **Network and Sharing Center**
- Click on **Change adapter settings** and Click **Open**.
- Right-click on your local adapter and select **Properties**.
- In the Local Area Connection Properties window select **Internet Protocol Version 6 (TCP/IPv6)** then click the **Properties** button.
- Enter **Default Gateway** and click **OK**.



Verify IPv6 Address on Windows Computer

C:\> **ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . : **2001:1111::10**

Link-local IPv6 Address . . . . : fe80::449d:6a9a:2c80:80dc%64

Default Gateway . . . . : **2001:1111::1**

C:\>

Assigning IPv6 Address on Linux Computer

bt ~ # **route -6 add default gw 2001:1111::1**

Verify IPv6 Address on Linux Computer

bt ~ # **route -6**

Kernel IPv6 routing table

Destination	Next Hop	Flag	Met	Ref	Use	If
::1/128	::	Un	0	1	0	lo
2001:1111::/64	::	U	256	0	2	eth0
fe80::468a:5bff:fed4:3899/128	::	Un	0	1	0	lo
fe80::/64	::	U	256	0	0	eth0
ff00::/8	::	U	256	0	0	eth0
::/0	**2001:1111::1**	**UG**	**1**	**0**	**0**	**eth0**

bt ~ #

Internal Components of Router

ZOOM TECHNOLOGIES

- **ROM (Read only Memory)**
  - **It contains a bootstrap program which searches and loads the operating system.**
  - **It is similar to the BIOS of a PC.**
  - **It also contains a ROMMON for advance troubleshooting.**

- **Flash memory**
  - **The Internetwork Operating System (IOS) is stored here.**
  - **IOS is a Cisco proprietary operating system.**

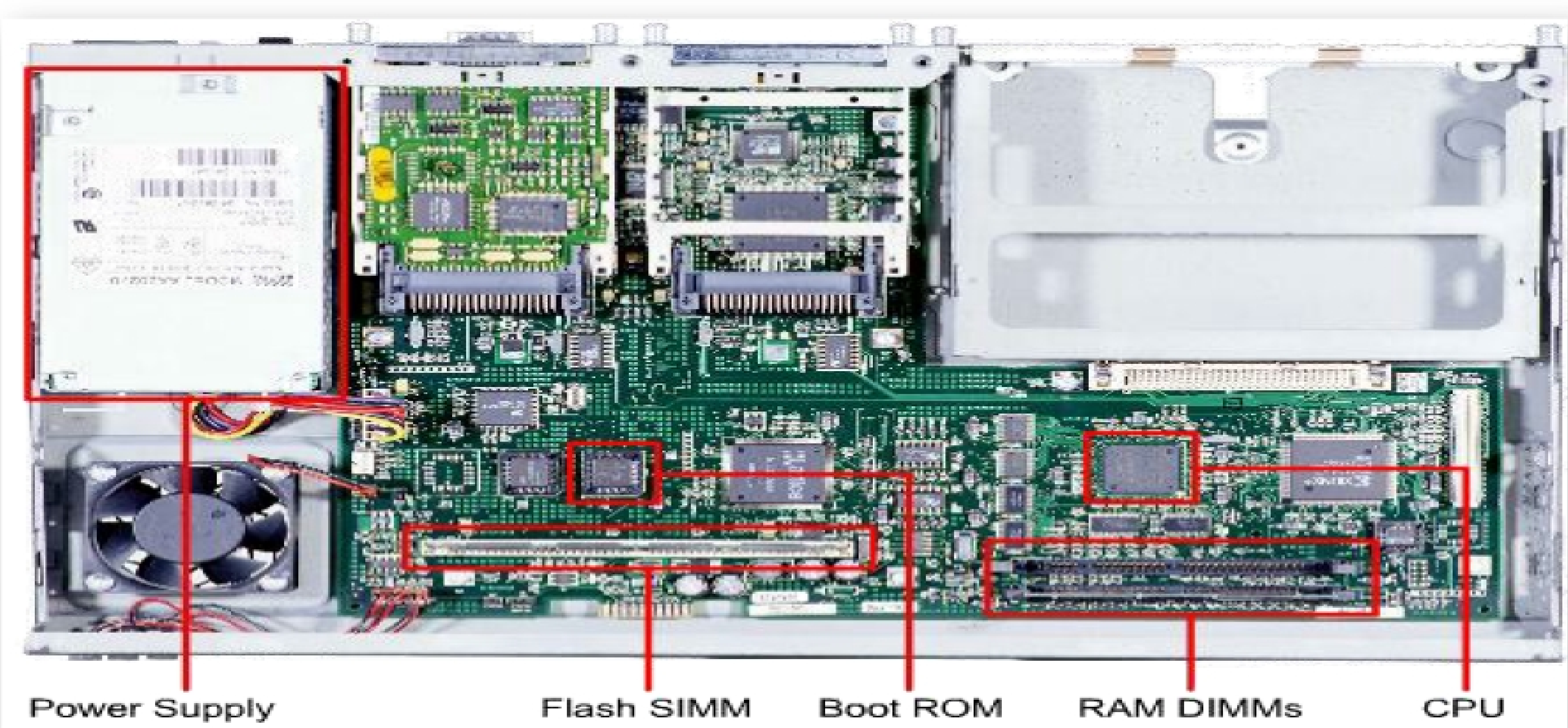
CCIE CCNP CCNA

Internal Components of Router

- NVRAM (Non Volatile Random Access Memory)
  - NVRAM is similar to a hard disk.
  - It is also known as permanent storage.
  - The startup configuration is stored here.

- RAM (Random Access Memory)
  - It is also called as the main memory.
  - It is a temporary storage.
  - The running configuration is stored here.

Internal Components of Router



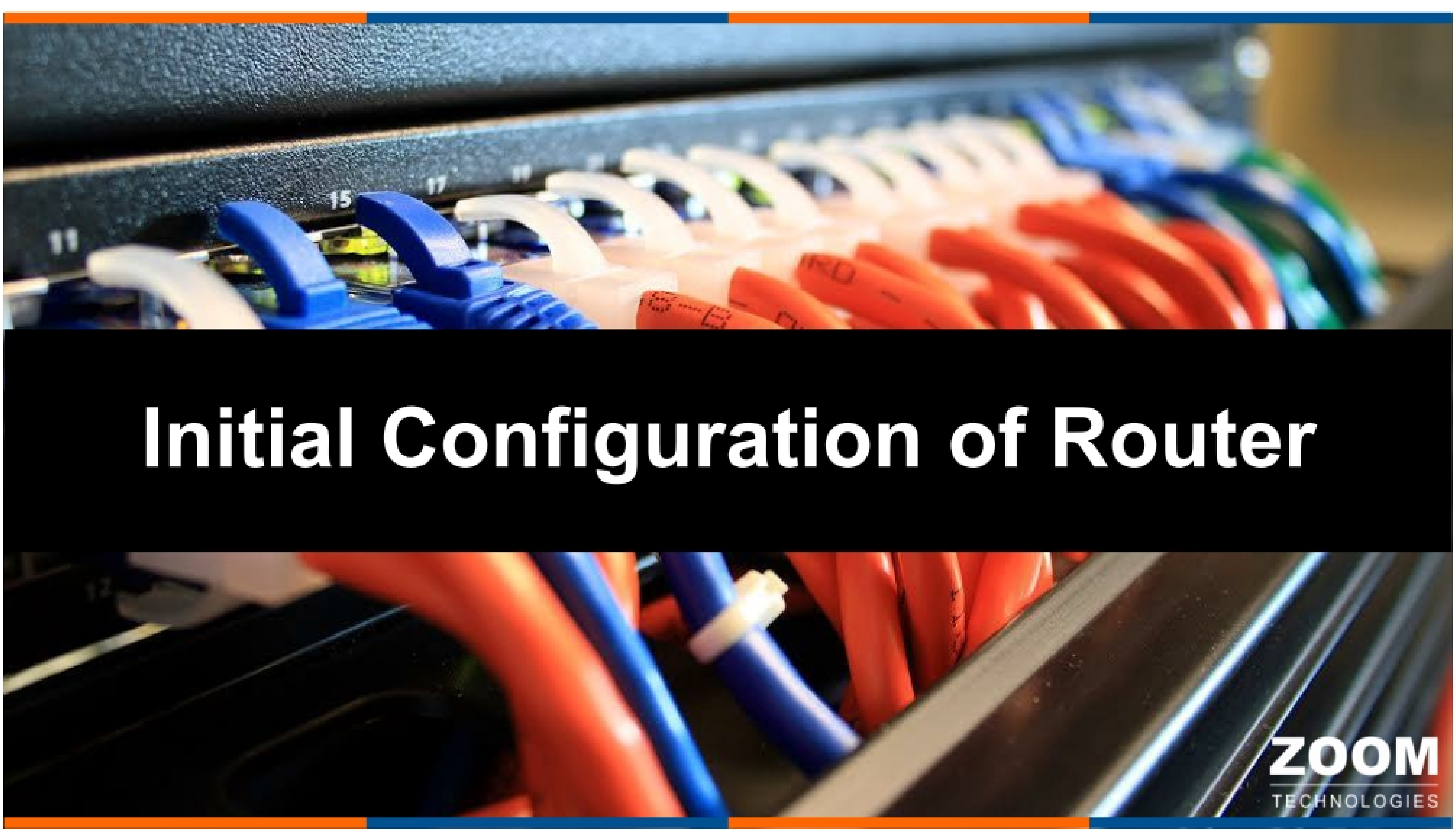
BOOT Sequence

ZOOM TECHNOLOGIES

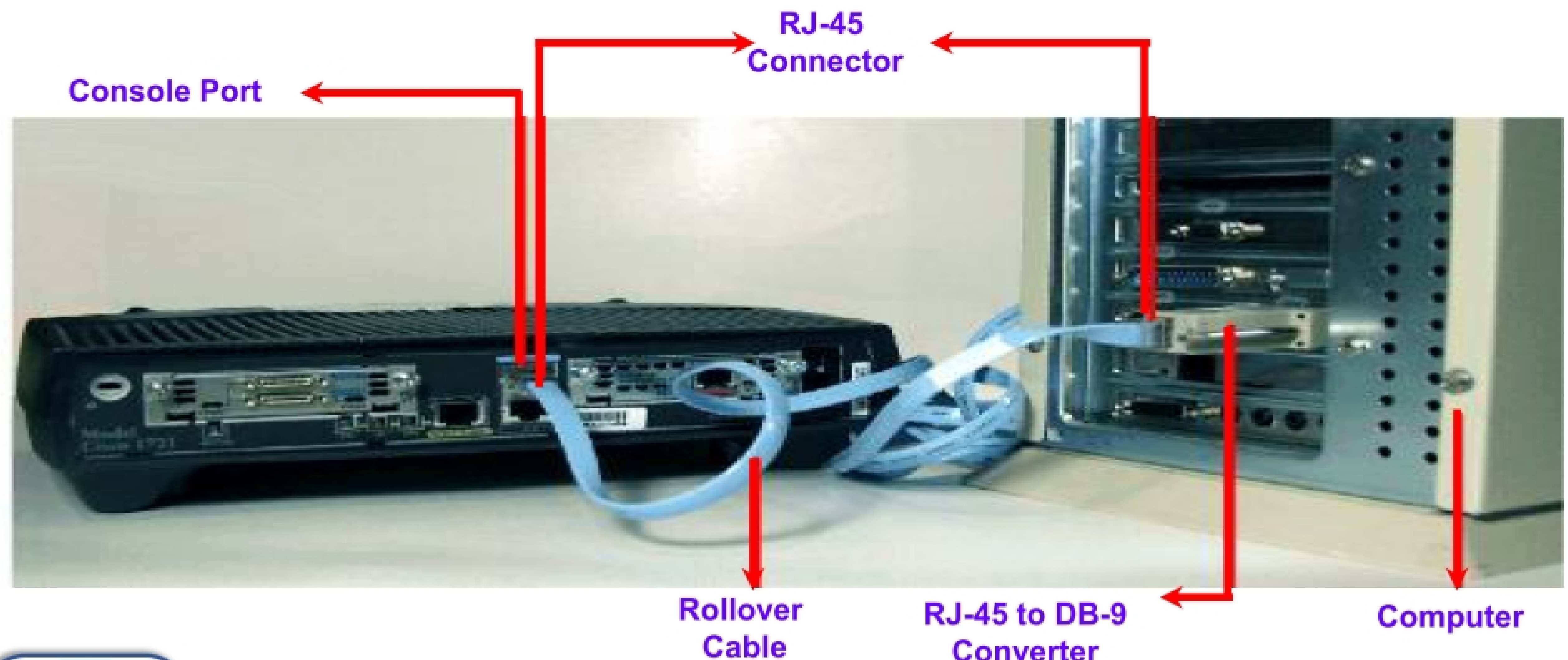
Power On Self Test – checks the hardware	POST
ROM loads Bootstrap program and searches for the IOS	ROM
IOS from Flash is loaded	FLASH
The startup configuration is loaded from the NVRAM	NVRAM
Boot process is completed as everything is loaded into the RAM	RAM

Configuration Register - 0x2102

CCIE CCNP CCNA



Console Connectivity



Access Router through Console

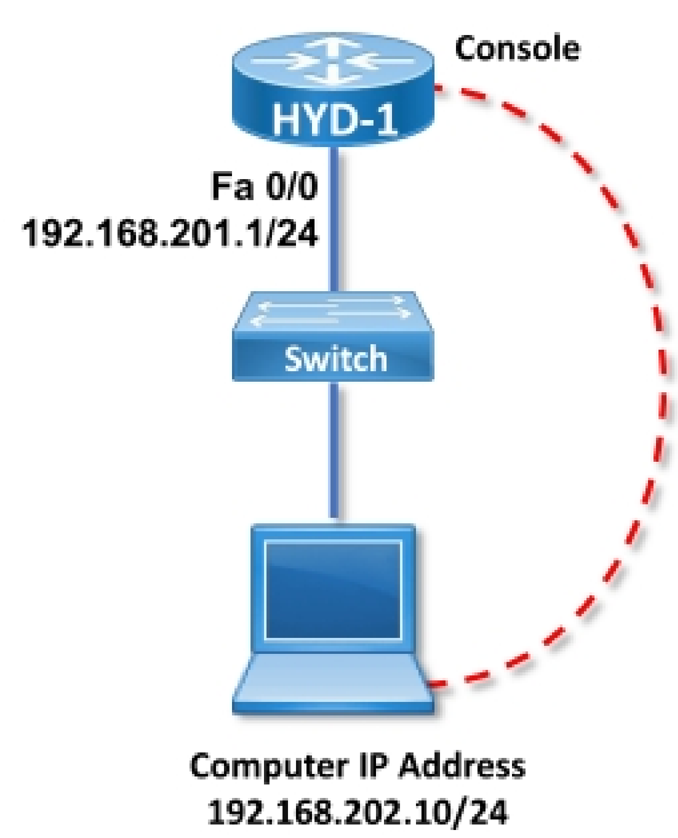
- **Cisco Routers and Switches do not have any default IP address or Configuration, hence its required to use the Console port for Initial Configuration.**
- **Require physical connection between the Cisco Router/Switch and PC via console cable.**

Emulation Software

- **WINDOWS**
- **Hyper-terminal / Putty / Teraterm**

- **LINUX**
- **Minicom -s**

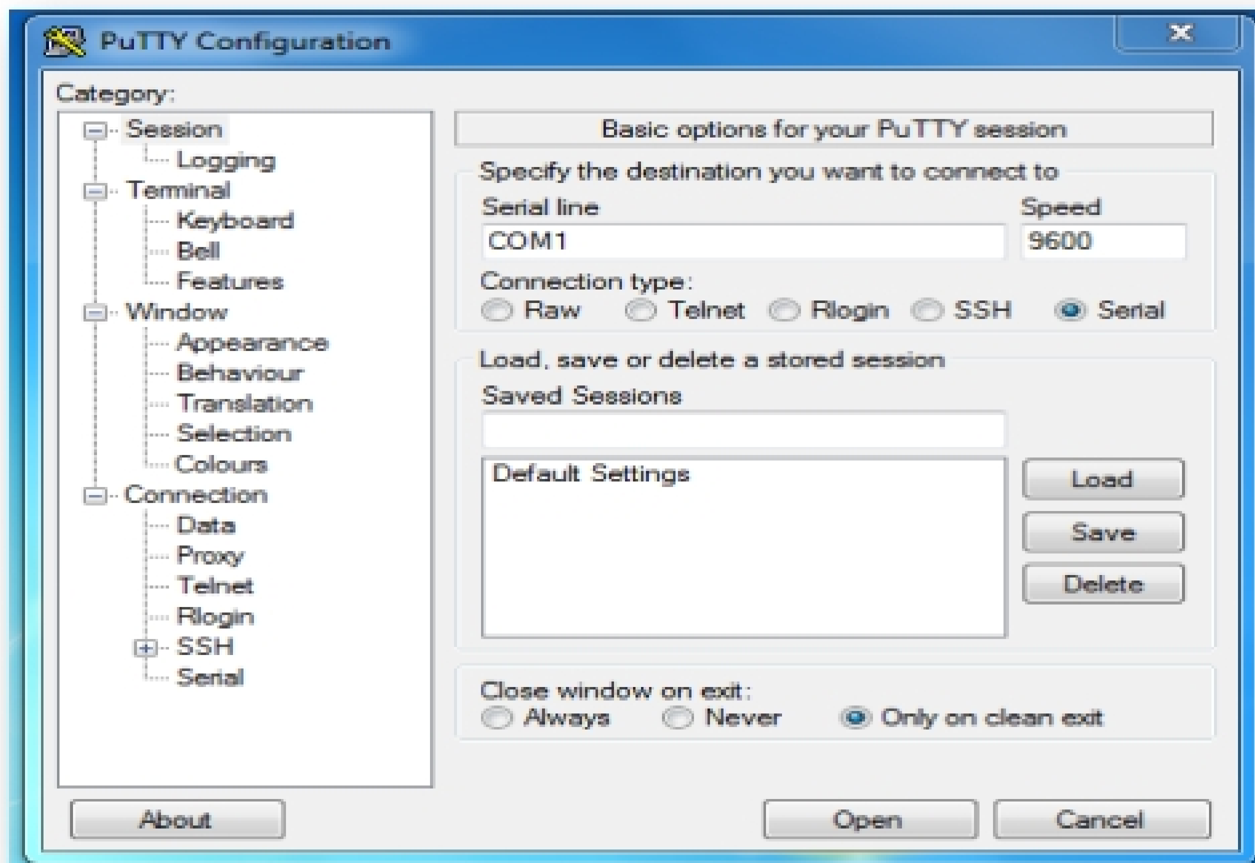
Initial Configuration



Access Router through Console

ZOOM TECHNOLOGIES

- Accessing router via console from Microsoft Windows Computer
- Start a terminal emulator application, such as PUTTY.exe
- Select Serial option and set speed to 9600
- Click Open



CCIE CCNP CCNA

Modes of the Router

ZOOM TECHNOLOGIES

- Setup Mode
- User Mode
- Privileged Mode
- Global Configuration Mode
- Interface Mode
- Line Mode

CCIE CCNP CCNA

Setup Mode

- The router enters in to the setup mode if the NVRAM is empty.

Router

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
```

User Mode

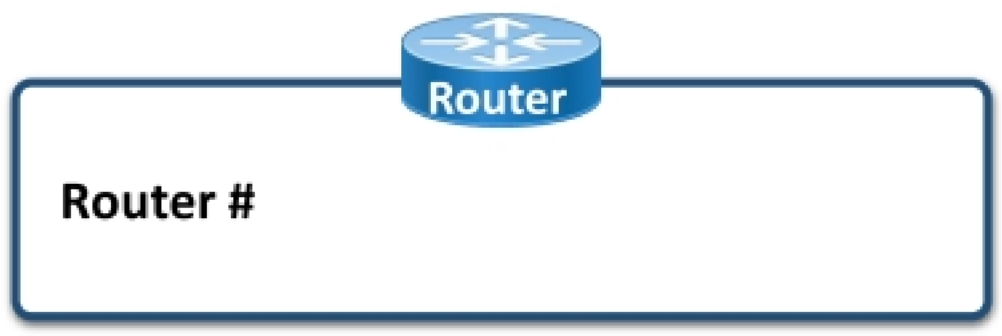
- Only some basic monitoring and limited show commands works in this mode.
  - Example of commands : enable, ping, traceroute, etc.

Router

```
Router >
```

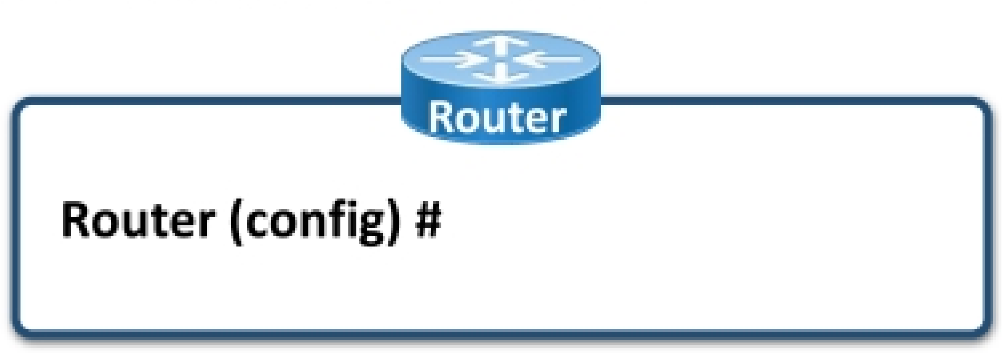
Privilege Mode

- Monitoring, Troubleshooting and Verification commands works in this mode.
  - Example of commands : show, configure terminal, write, etc.



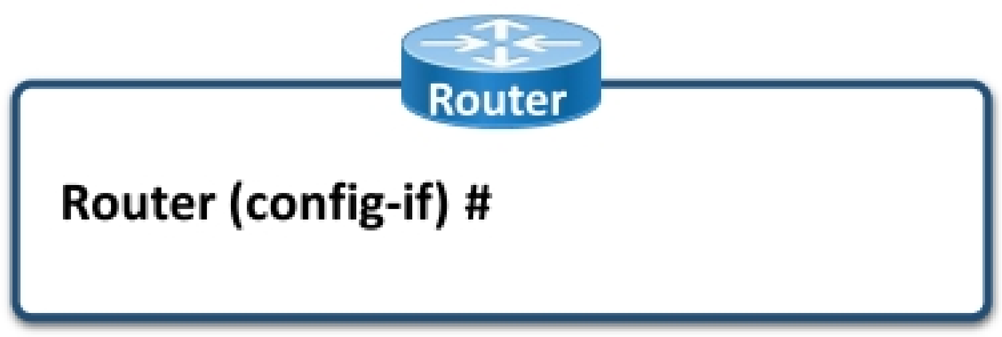
Global Configuration Mode

- Configuration changes made in this mode affects the operation of the device as a whole.
  - Example of commands : hostname, etc.



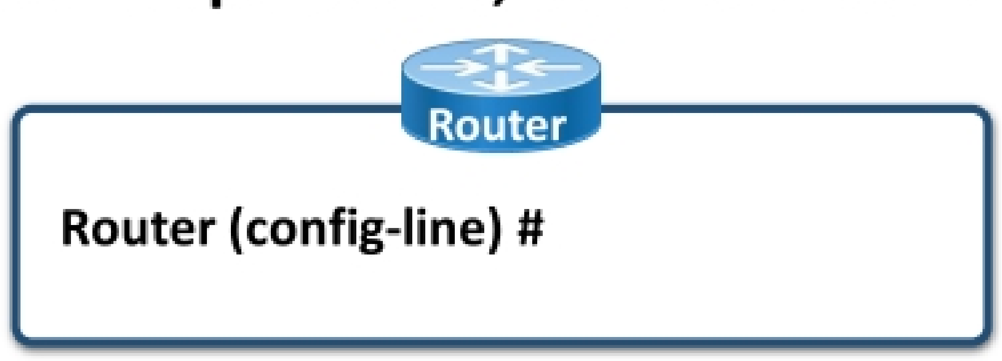
Interface Mode

- Commands given in this mode will apply to a specific network interface. i.e. FastEthernet 0/0 or Serial 0/0
  - Example of commands : ip address, no shutdown etc.

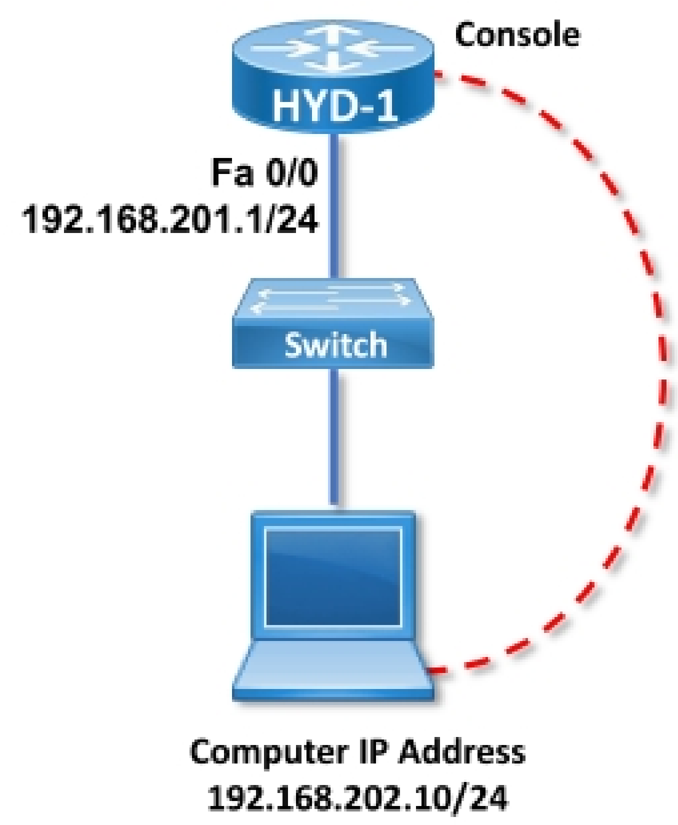


Line mode

- Commands given in this mode will apply to a specific physical or virtual lines. i.e. Console, Auxiliary or VTY.
  - Example of commands : password, no shutdown etc.



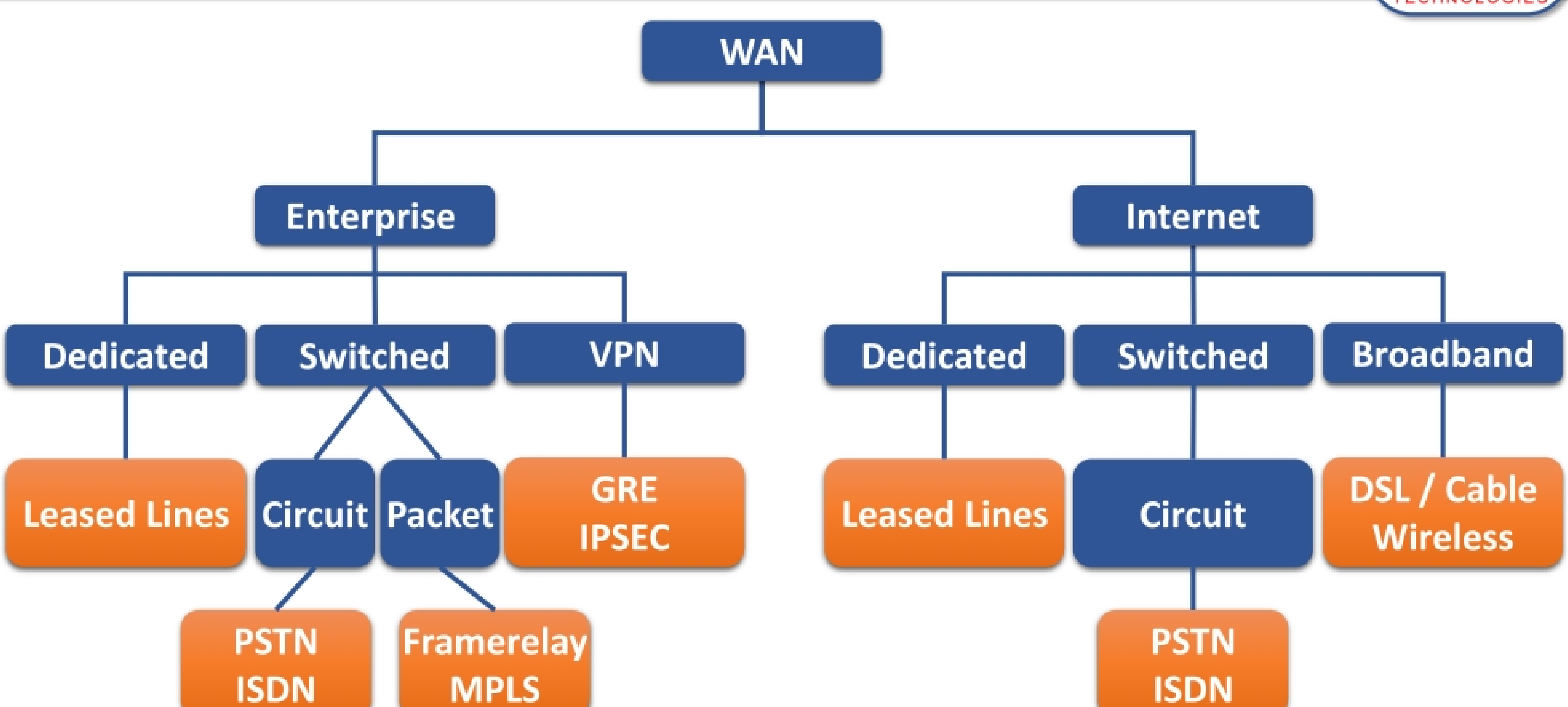
Accessing Router

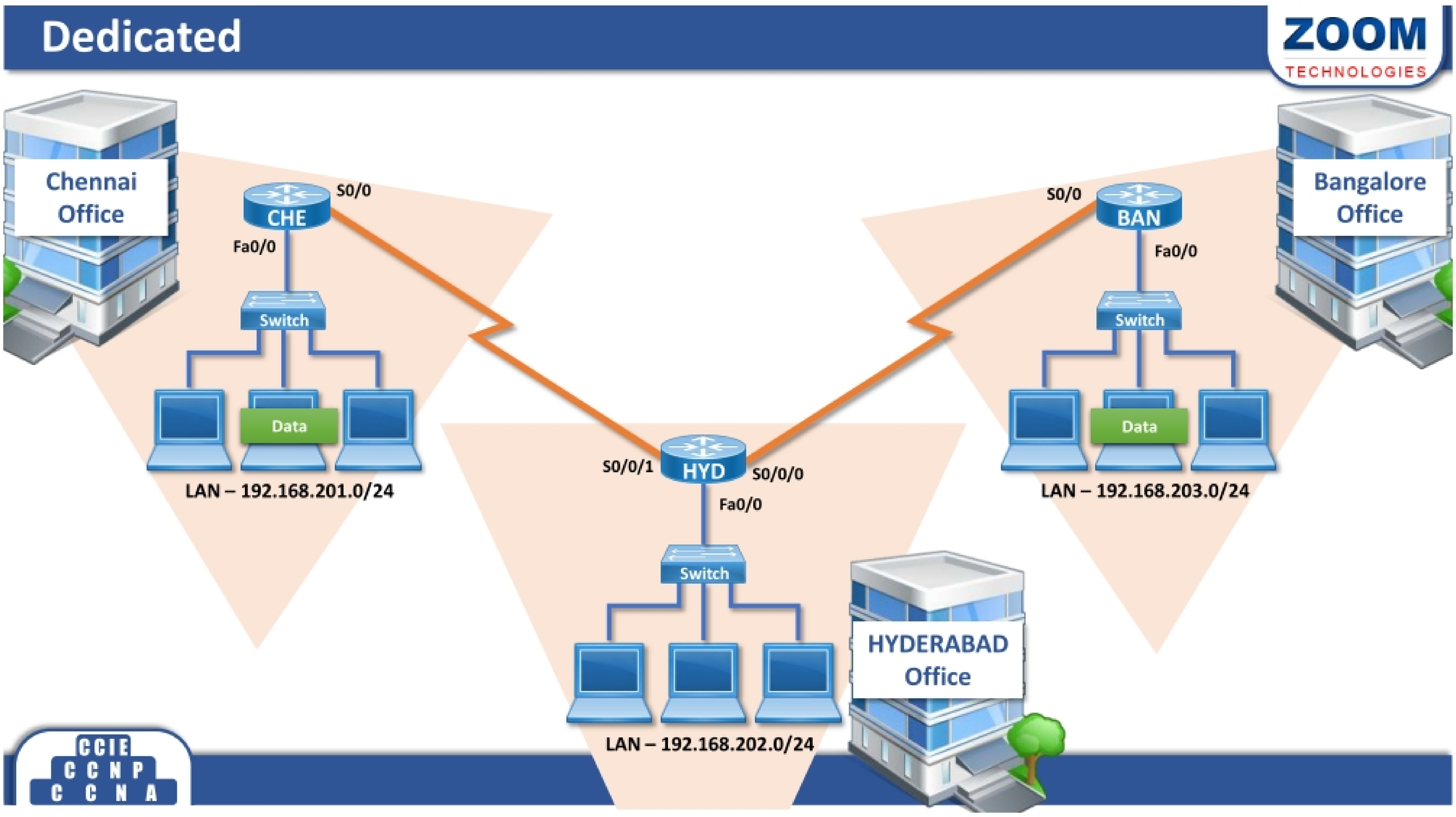


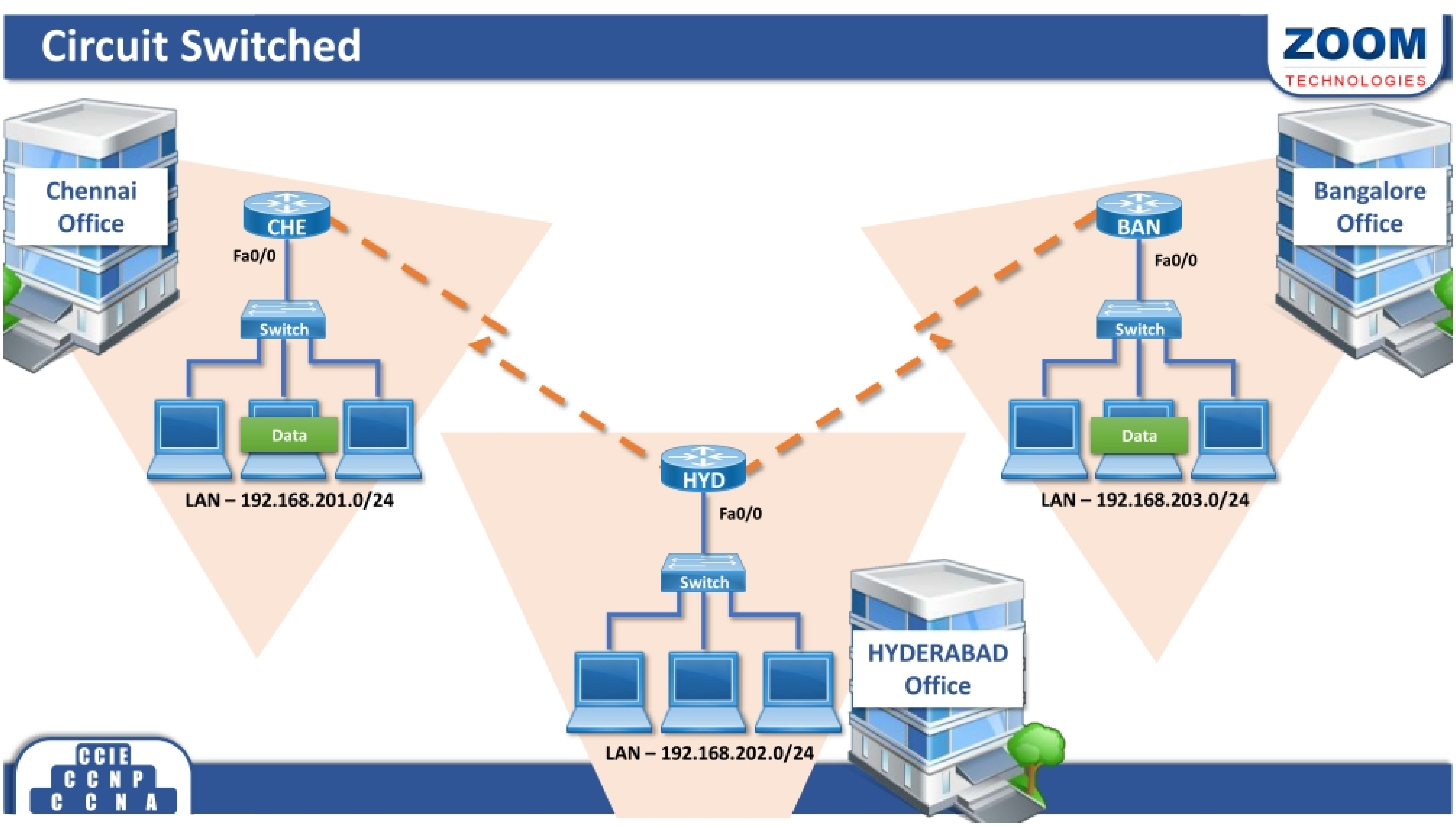
Types of Network Access

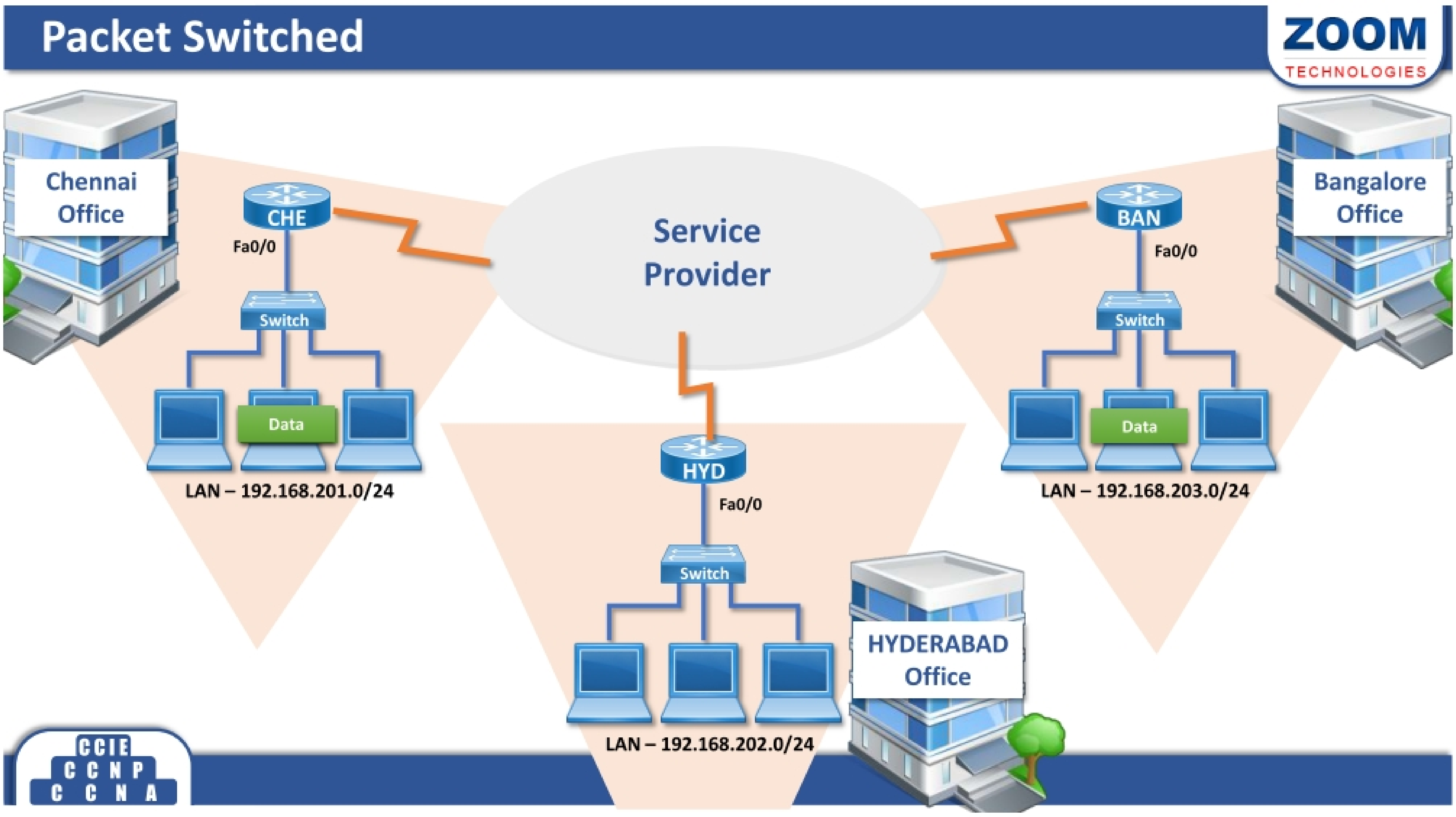
- **Enterprise Access**
- **Internet Access**

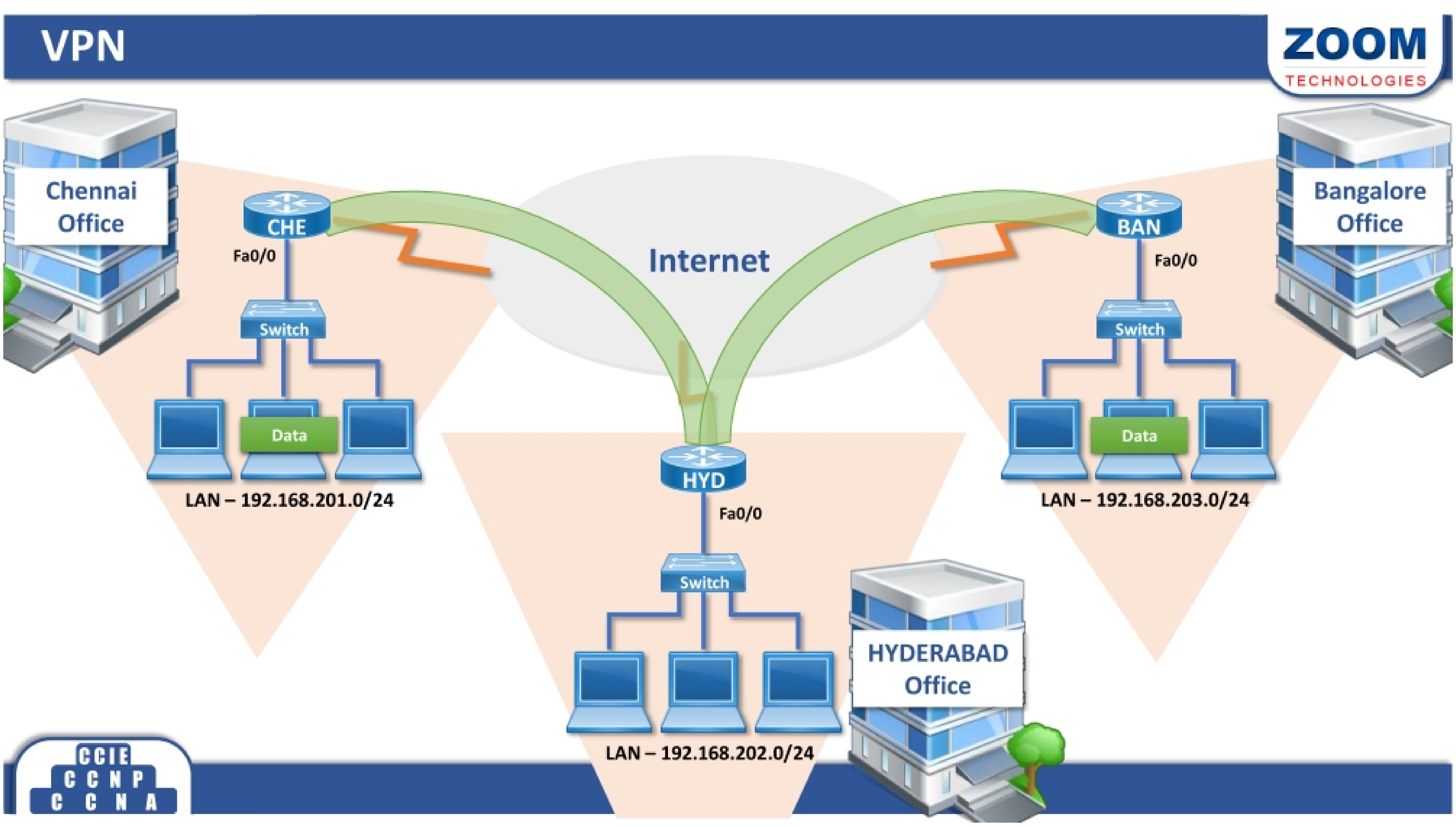
Types of WAN Technologies



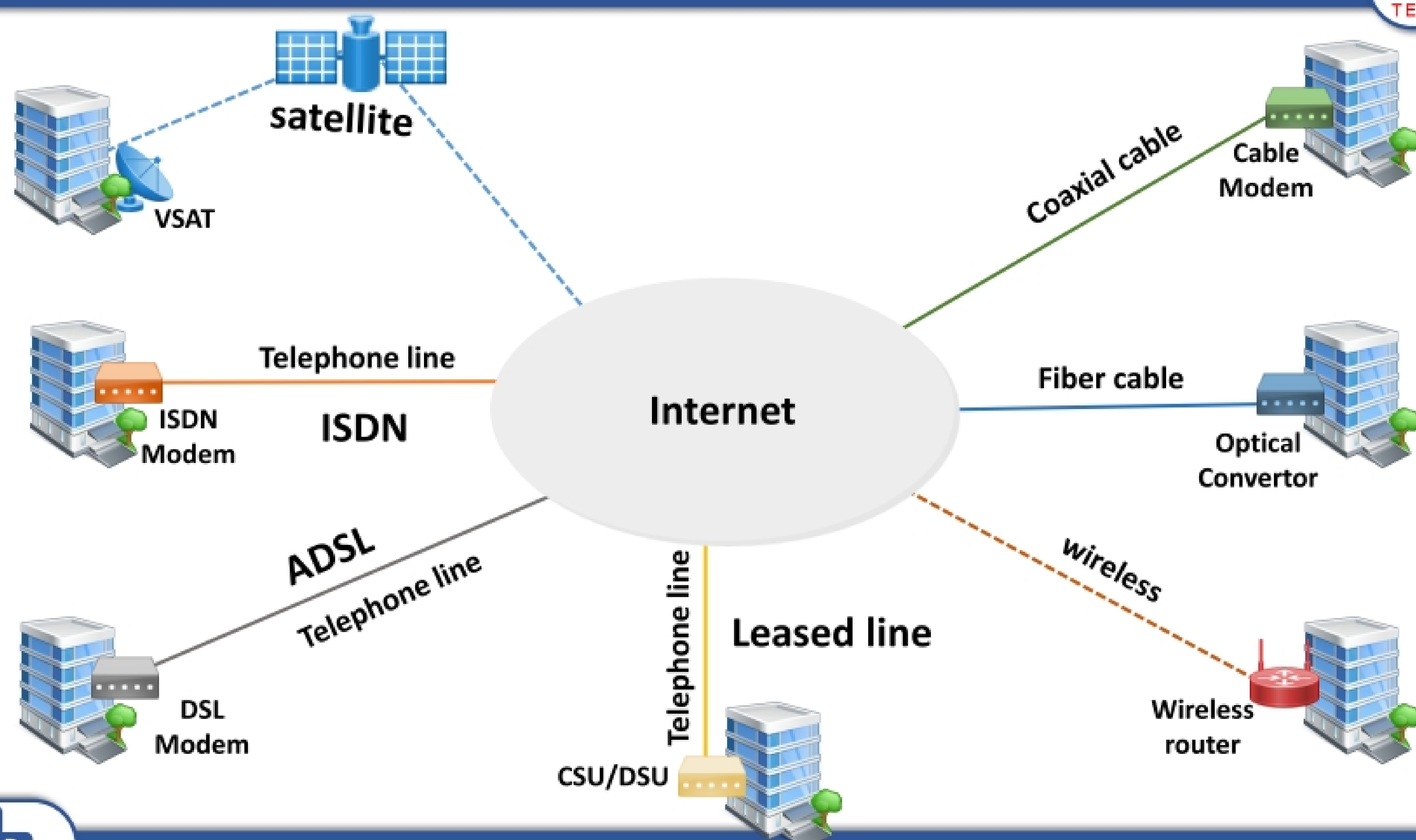

Dedicated
ZOOM
TECHNOLOGIES
Chennai Office
CHE
S0/0
Fa0/0
Switch
Data
LAN – 192.168.201.0/24
Bangalore Office
BAN
S0/0
Fa0/0
Switch
Data
LAN – 192.168.203.0/24
HYD
S0/0/1
S0/0/0
Fa0/0
Switch
LAN – 192.168.202.0/24
HYDERABAD Office
CCIE
CCNP
CCNA


Circuit Switched
ZOOM
TECHNOLOGIES
Chennai Office
CHE
Fa0/0
Switch
Data
LAN – 192.168.201.0/24
Bangalore Office
BAN
Fa0/0
Switch
Data
LAN – 192.168.203.0/24
HYD
Fa0/0
Switch
LAN – 192.168.202.0/24
HYDERABAD Office
CCIE
CCNP
CCNA


Packet Switched
ZOOM
TECHNOLOGIES
Chennai Office
CHE
Fa0/0
Switch
Data
LAN – 192.168.201.0/24
Service Provider
Bangalore Office
BAN
Fa0/0
Switch
Data
LAN – 192.168.203.0/24
HYD
Fa0/0
Switch
LAN – 192.168.202.0/24
HYDERABAD Office
CCIE
CCNP
CCNA

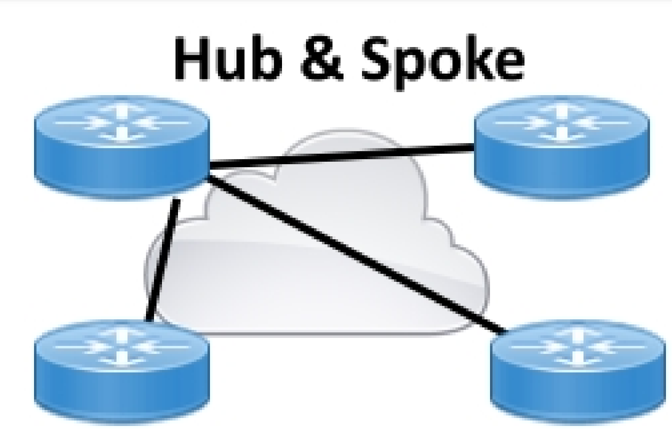

VPN
ZOOM
TECHNOLOGIES
Chennai Office
CHE
Fa0/0
Switch
Data
LAN – 192.168.201.0/24
Internet
Bangalore Office
BAN
Fa0/0
Switch
Data
LAN – 192.168.203.0/24
HYD
Fa0/0
Switch
LAN – 192.168.202.0/24
HYDERABAD Office
CCIE
CCNP
CCNA

Internet Connectivity

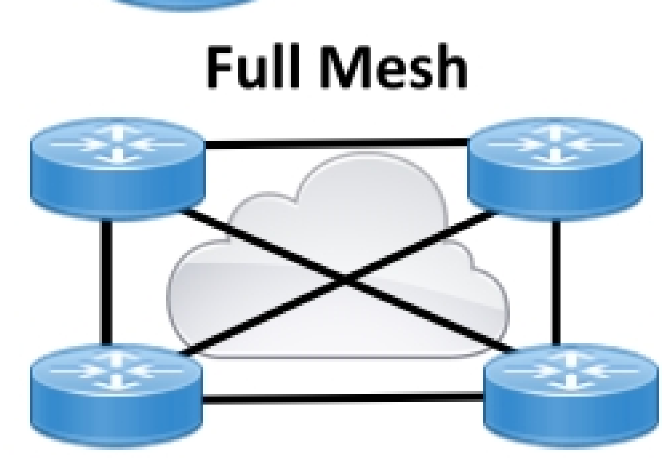


WAN Topologies

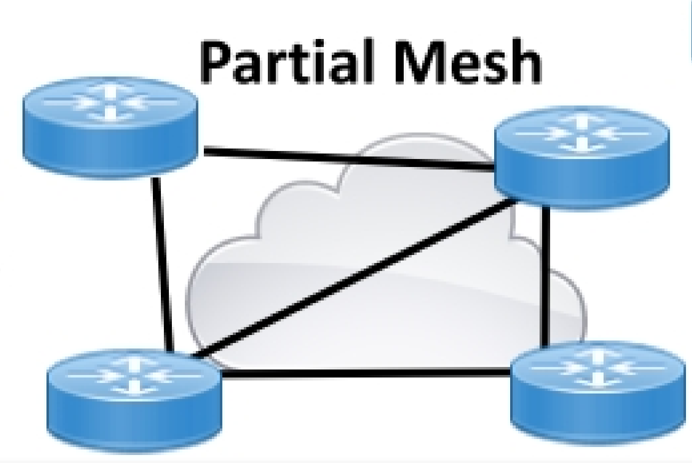
- STAR or Hub and Spoke Topology
  - Easy to deploy, Less number of connections
  - No backup/redundancy



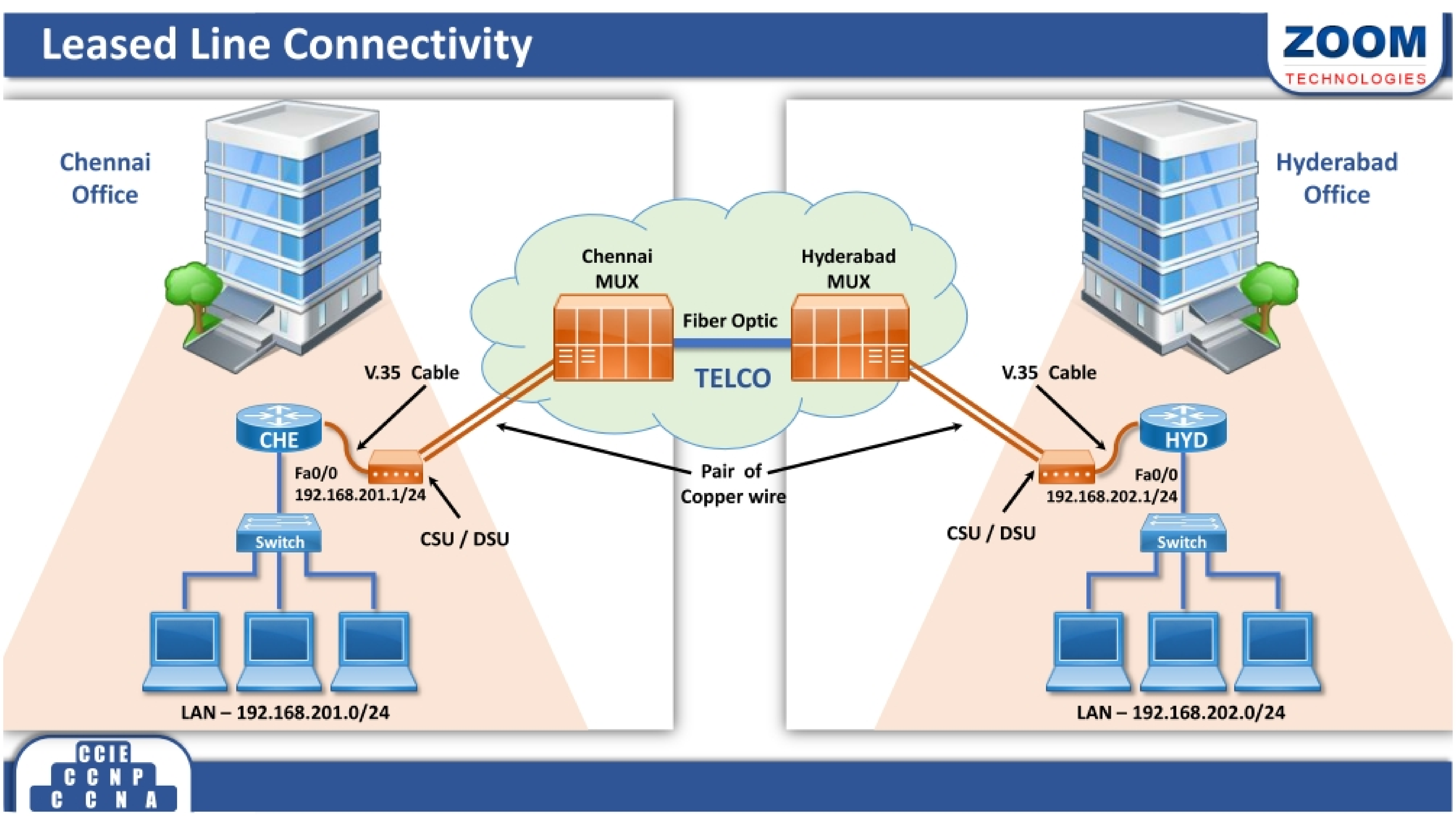
- Full Mesh Topology
  - All branches interconnected, full redundancy
  - More connections, complex configuration



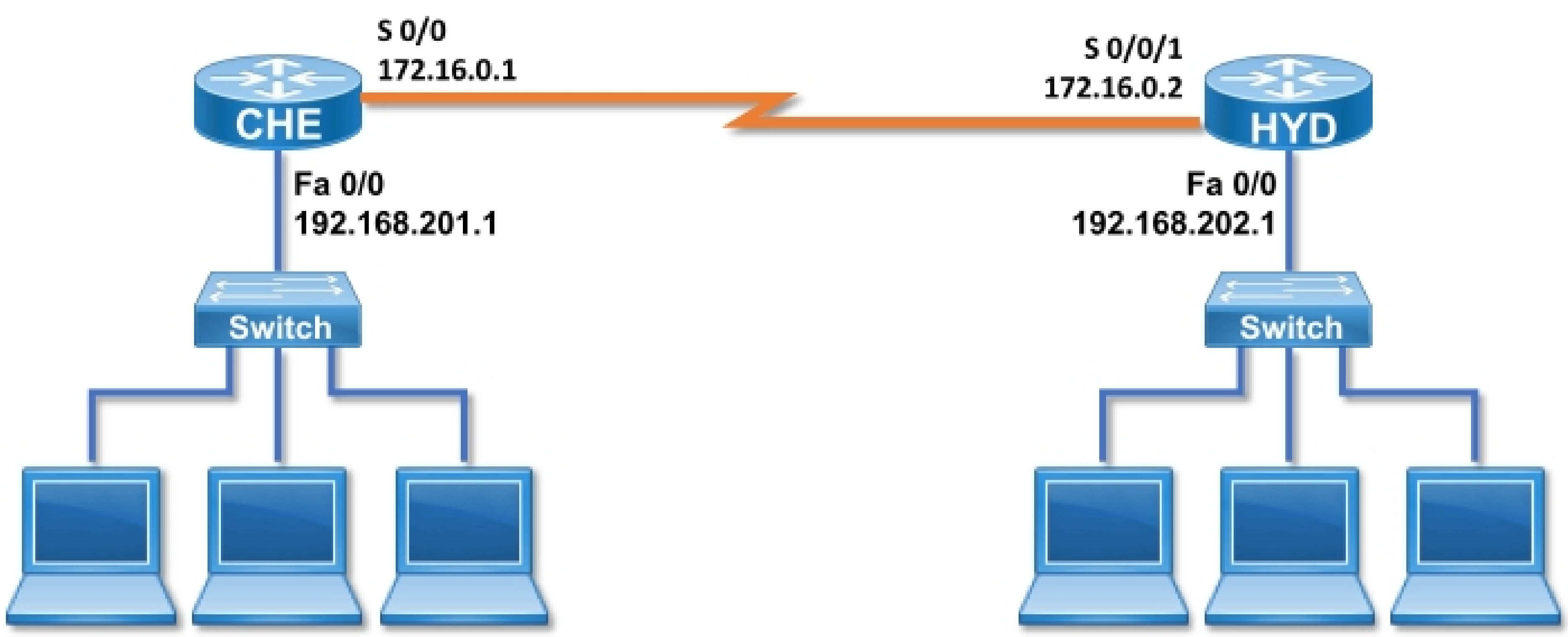
- Partial Mesh Topology
  - Mix of Star & Full mesh topologies




WAN Connectivity
ZOOM
TECHNOLOGIES


Leased Line Connectivity
ZOOM
TECHNOLOGIES
Chennai Office
Hyderabad Office
Chennai MUX
Hyderabad MUX
Fiber Optic
TELCO
V.35 Cable
V.35 Cable
CHE
HYD
Fa0/0
192.168.201.1/24
Fa0/0
192.168.202.1/24
Pair of Copper wire
CSU / DSU
CSU / DSU
Switch
Switch
LAN – 192.168.201.0/24
LAN – 192.168.202.0/24
CCIE
CCNP
CCNA

Wan Connectivity Representation



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16

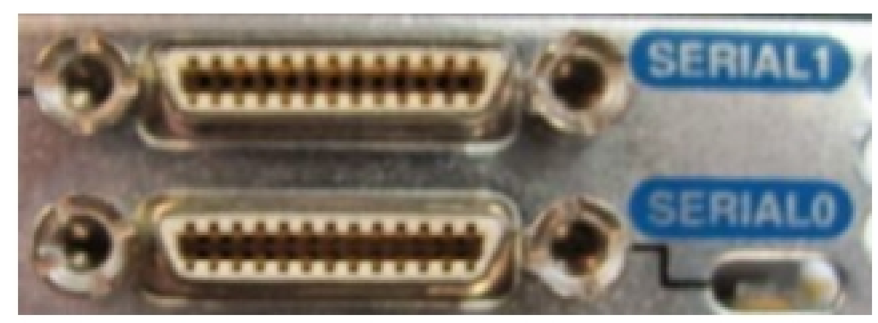
Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/1	172.16.0.0/16

Device Classification

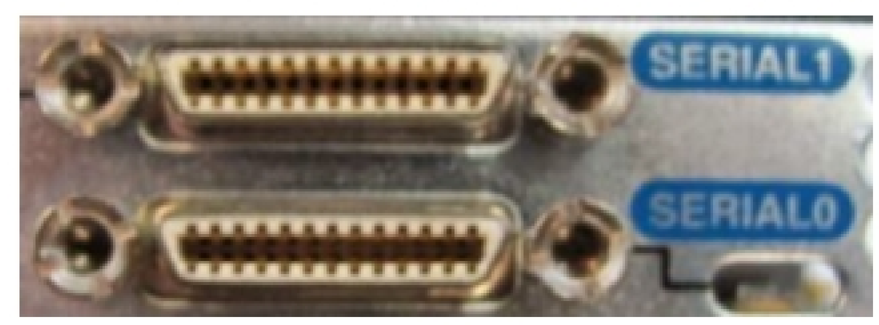
DCE	DTE
• Data Communication Equipment • Generate clocking (i.e. Speed) • Master • Example of DCE:- CSU/DSU	• Data Termination Equipment • Accept clocking (i.e. Speed) • Slave • Example of DTE:- Router

Serial - back to back cable

- When the distance between two Routers is short, a special V.35 Back to Back Cable is used to replace the copper wire, CSU/DSU and MUX.
- For data communication using back to back Serial cable, one end has to be a DCE and the other has to be a DTE.



ROUTER 1



ROUTER 2

Encapsulation

- Encapsulation is the process of adding a new Header or Trailer to data.
- The header and trailer contains information which is needed for proper transportation of the data.
- There are different types of WAN Encapsulation:
  - PPP
  - HDLC

Wan Encapsulation

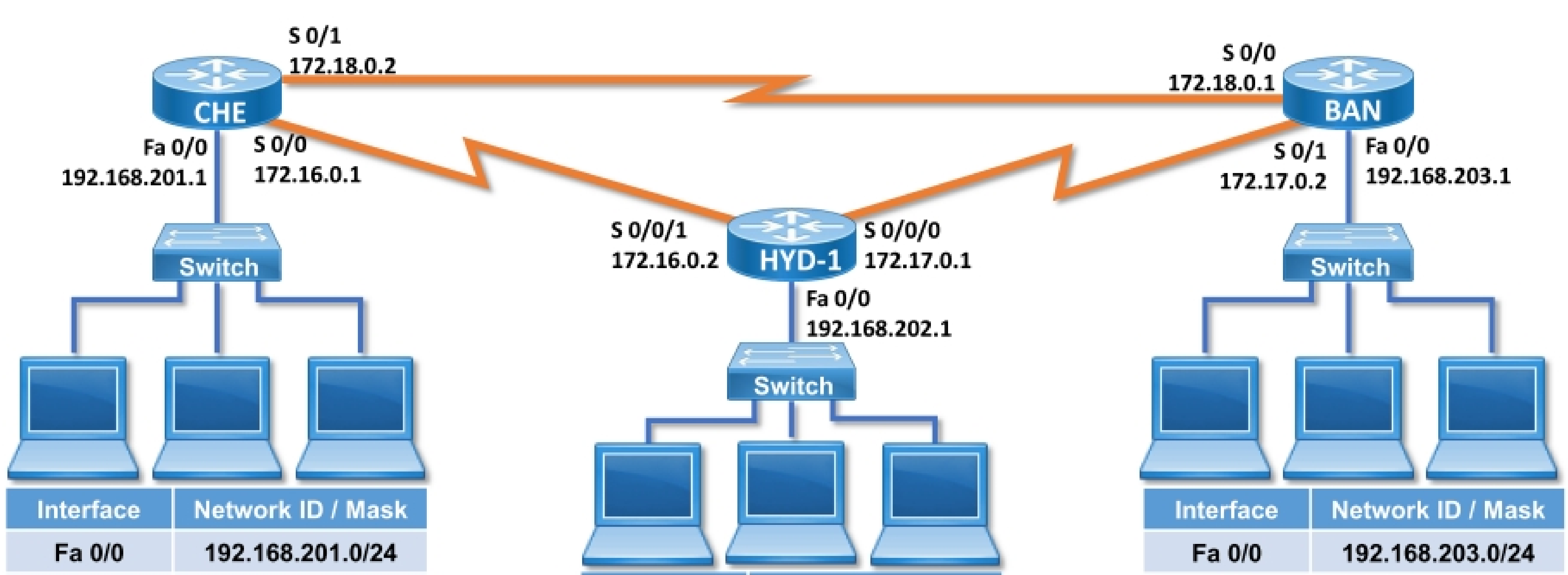
ZOOM TECHNOLOGIES

PPP	HDLC
• Point to Point Protocol • Open Standard Protocol • Supports Authentication • Supports Compression	• High level Data link Control • Vendor proprietary Protocol • No Support for Authentication • No Support for Compression

CCIE CCNP CCNA

Wan - Serial Interface Configuration on IPv4 Network

ZOOM TECHNOLOGIES



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16
S 0/1	172.18.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	172.17.0.0/16
S 0/0/1	172.16.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	172.18.0.0/16
S 0/1	172.17.0.0/16

CCIE CCNP CCNA

Identify Serial Interface (DCE or DTE)

Router# show controllers serial < no. >

Wan - Serial Interface Configuration on IPv4 Network

Router (config) # interface Serial <no.>

Router (config-if) # ip address < ip address > < subnet mask >

Router (config-if) # no shutdown

Router (config-if) # clock rate < bandwidth >

Router (config-if) # encapsulation < HDLC/PPP >

Wan - Serial Interface Configuration on IPv4 Network

CHE

```
CHE (config)# interface serial 0/0
CHE (config-if)# ip address 172.16.0.1 255.255.0.0
CHE (config-if)# no shutdown
CHE (config-if)# clock rate 64000
CHE (config-if)# encapsulation hdlc
CHE (config-if)# exit
CHE (config)# interface serial 0/1
CHE (config-if)# ip address 172.18.0.2 255.255.0.0
CHE (config-if)# no shutdown
CHE (config-if)# encapsulation hdlc
CHE (config-if)# exit
```

BAN

```
BAN (config)# interface serial 0/0
BAN (config-if)# ip address 172.18.0.1 255.255.0.0
BAN (config-if)# no shutdown
BAN (config-if)# clock rate 64000
BAN (config-if)# encapsulation hdlc
BAN (config-if)# exit
BAN (config)# interface serial 0/1
BAN (config-if)# ip address 172.17.0.2 255.255.0.0
BAN (config-if)# no shutdown
BAN (config-if)# encapsulation hdlc
BAN (config-if)# exit
```

HYD-1

```
HYD-1 (config)# interface serial 0/0/0
HYD-1 (config-if)# ip address 172.17.0.1 255.255.0.0
HYD-1 (config-if)# no shutdown
HYD-1 (config-if)# clock rate 64000
HYD-1 (config-if)# encapsulation hdlc
HYD-1 (config-if)# exit
HYD-1 (config)# interface serial 0/0/1
HYD-1 (config-if)# ip address 172.16.0.2 255.255.0.0
HYD-1 (config-if)# no shutdown
HYD-1 (config-if)# encapsulation hdlc
HYD-1 (config-if)# exit
```

Network Diagram

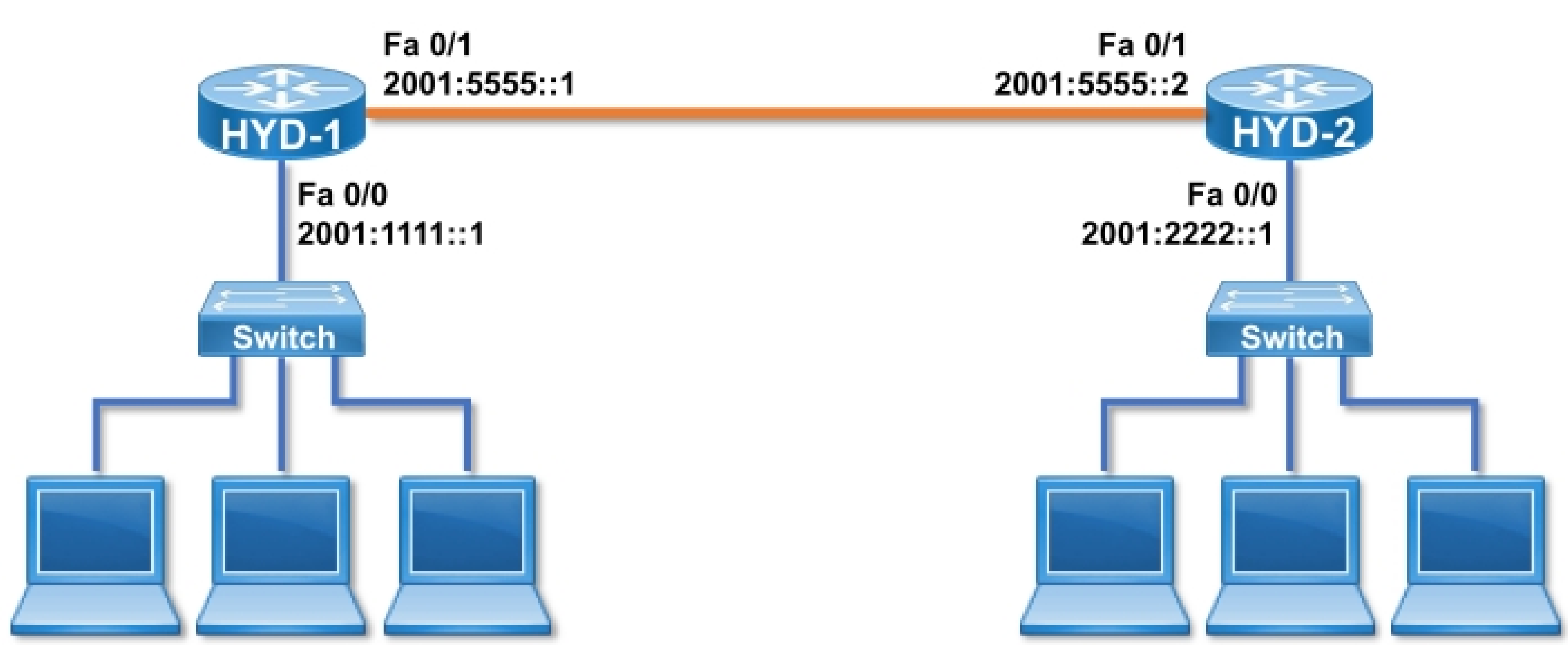
Wan - Serial Interface - Verification

Router # show interface serial <no. >

Troubleshooting Serial Interface

- Serial 0/0 is up , line protocol is up
  - Layer 1 and Layer 2 Connectivity and configuration is fine
- Serial 0/0 is administratively down, line protocol is down
  - 'No Shutdown' has to be given on the local Router's Serial interface
- Serial 0/0 is up, line protocol is down
  - Encapsulation mismatch or clock rate has not been given on the DCE interface or Lease Line problem
- Serial 0/0 is down, line protocol is down
  - Problem with the v.35 cable, CSU/DSU or 'no shutdown' has not been given on the remote Router

Wan - Ethernet Interface Configuration on IPv6 Network



Interface	Network ID / Mask
Fa 0/0	2001:1111::/64
Fa 0/1	2001:5555::/64

Interface	Network ID / Mask
Fa 0/0	2001:2222::/64
Fa 0/1	2001:5555::/64

Wan - Ethernet Interface Configuration on IPv6 Network

Router (config) # interface <ethernet> <no.>
Router (config-if) # ipv6 address < ip > < prefix length >
Router (config-if) # no shutdown

Wan - Ethernet Interface Configuration on IPv6 Network

HYD-1

```
HYD-1 (config)# interface fastethernet 0/1
HYD-1 (config-if)# ipv6 address 2001:5555::1/64
HYD-1 (config-if)# no shutdown
HYD-1 (config-if)# exit
HYD-1 (config)#
```

HYD-2

```
HYD-2 (config)# interface fastethernet 0/1
HYD-2 (config-if)# ipv6 address 2001:5555::2/64
HYD-2 (config-if)# no shutdown
HYD-2 (config-if)# exit
HYD-2 (config)#
```

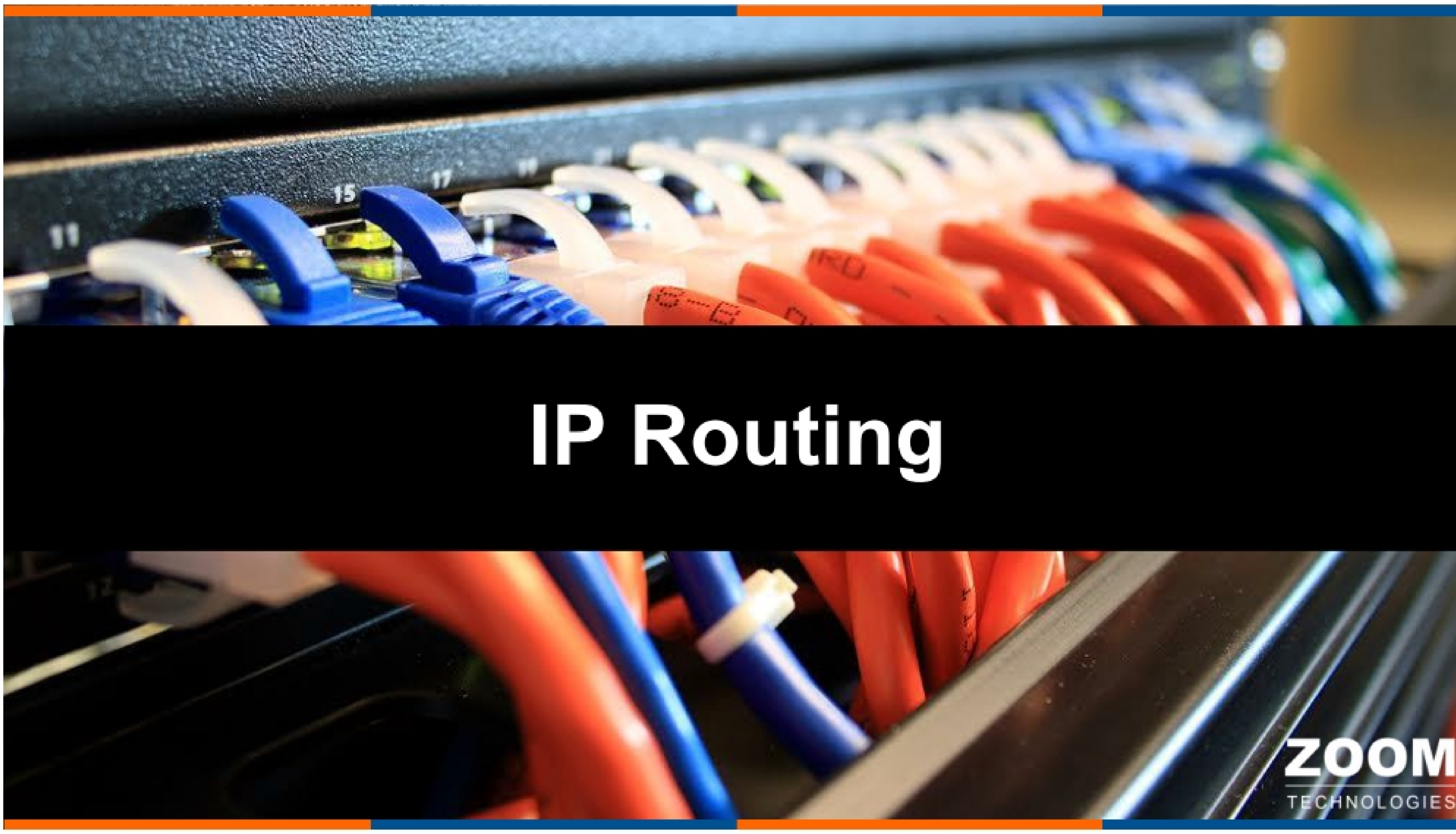
Network Diagram

Wan - Ethernet Interface - Verification

Router # show interface <ethernet> <no. >

Troubleshooting Ethernet Interface

- **Fastethernet 0/0 is up , line protocol is up**
  - **Layer 1 and Layer 2 Connectivity and configuration is fine**
- **Fastethernet 0/0 is administratively down, line protocol is down**
  - **'No Shutdown' has to be given on the local etherent interface**
- **Fastethernet 0/0 is up, line protocol is down**
  - **Speed & Duplex Mismatch or 'No Shutdown' has not been given on the remote device ethernet interface.**
- **Fastethernet 0/0 is down, line protocol is down**
  - **Layer 1 problem - No device attached or faulty cable.**



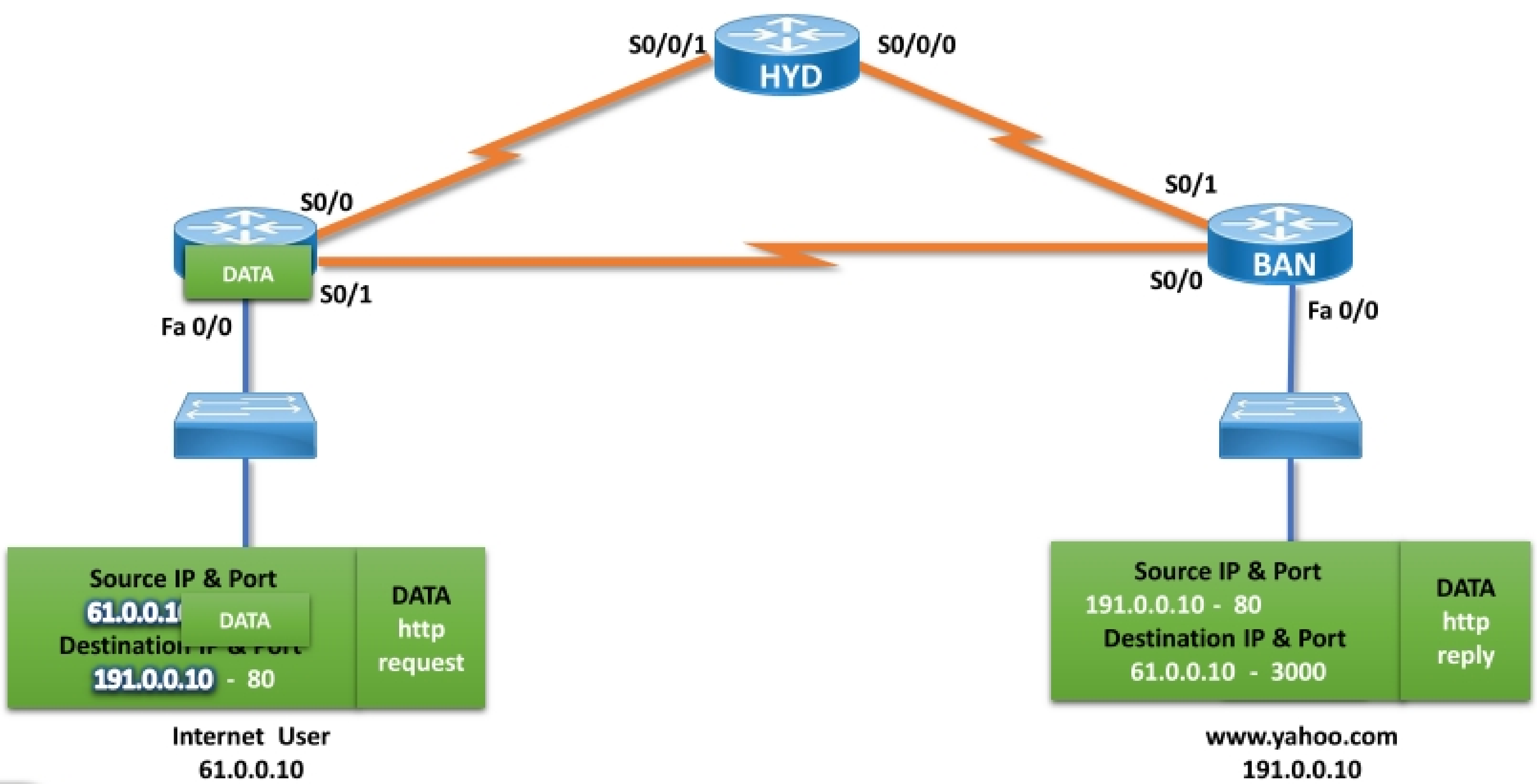
IP Routing

ZOOM TECHNOLOGIES

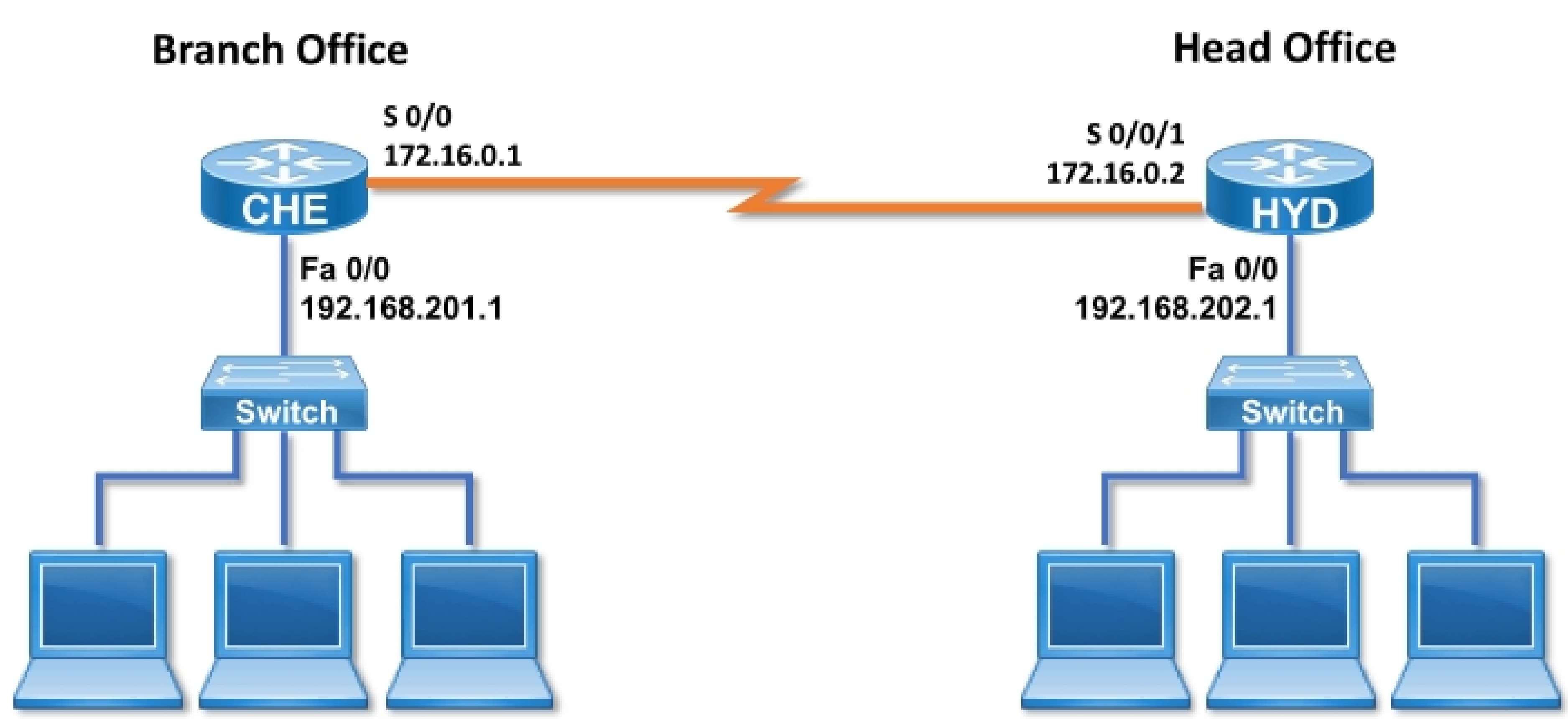
- **Routing is the process of moving IP packets from one network to another network.**
- **Routing involves two basic activities:**
  - **Determining the best paths.**
  - **Forwarding packets through these best paths.**

CCIE CCNP CCNA

IP Routing



IP Routing - Network Diagram



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16

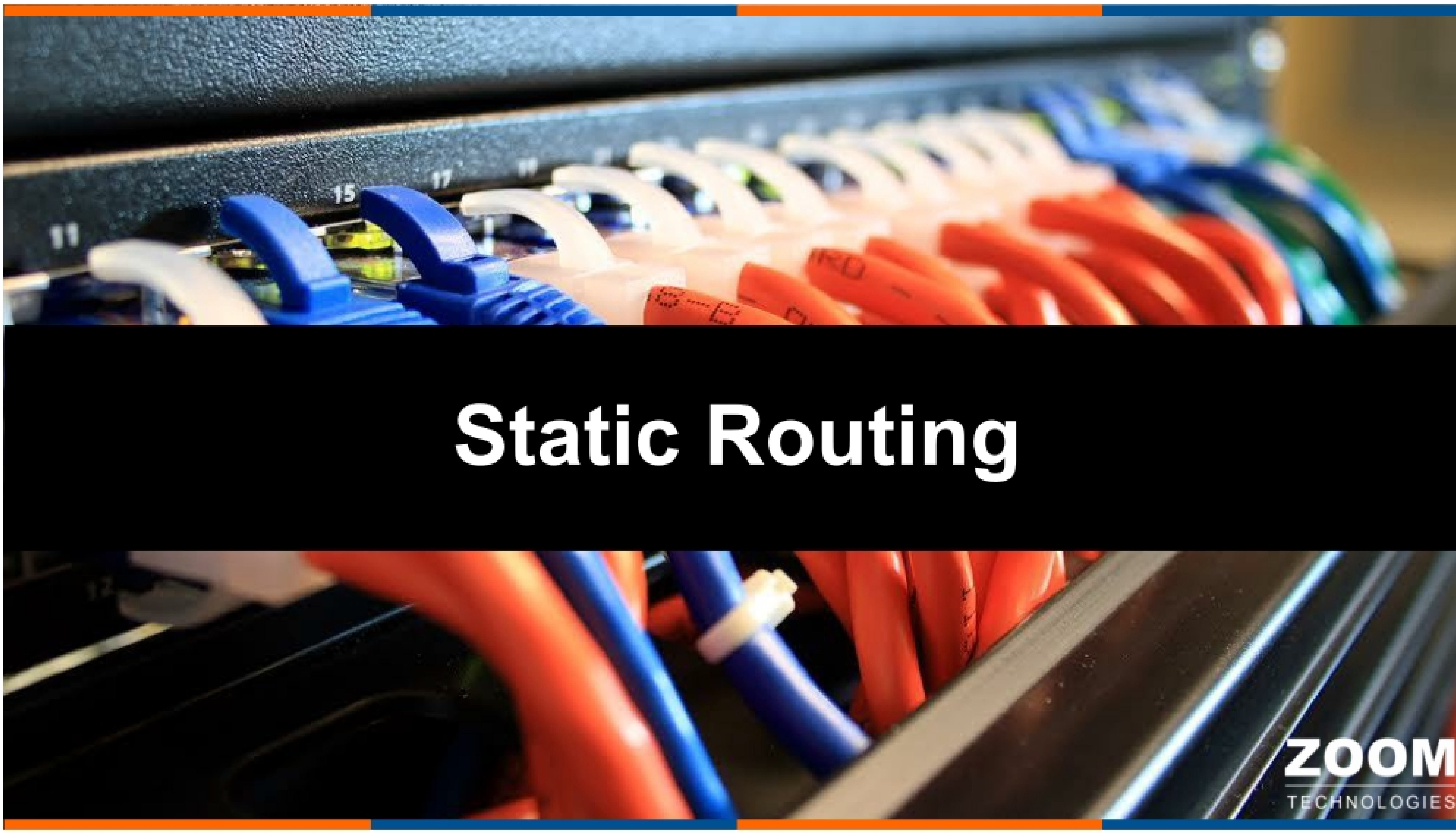
Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/1	172.16.0.0/16

Conditions for IP Routing

- The HO Router FastEthernet IP address should be in the same network as the HO LAN and similarly the BO Router FastEthernet IP address should belong to the same network as the BO LAN.
- The Serial interface IP between the HO and the BO should be in the same IP network.
- HO LAN and BO LAN should be in different IP network.
- All interfaces of a Router should be in different IP network.

Types of Routing

- Static Routing
- Dynamic Routing
- Default Routing

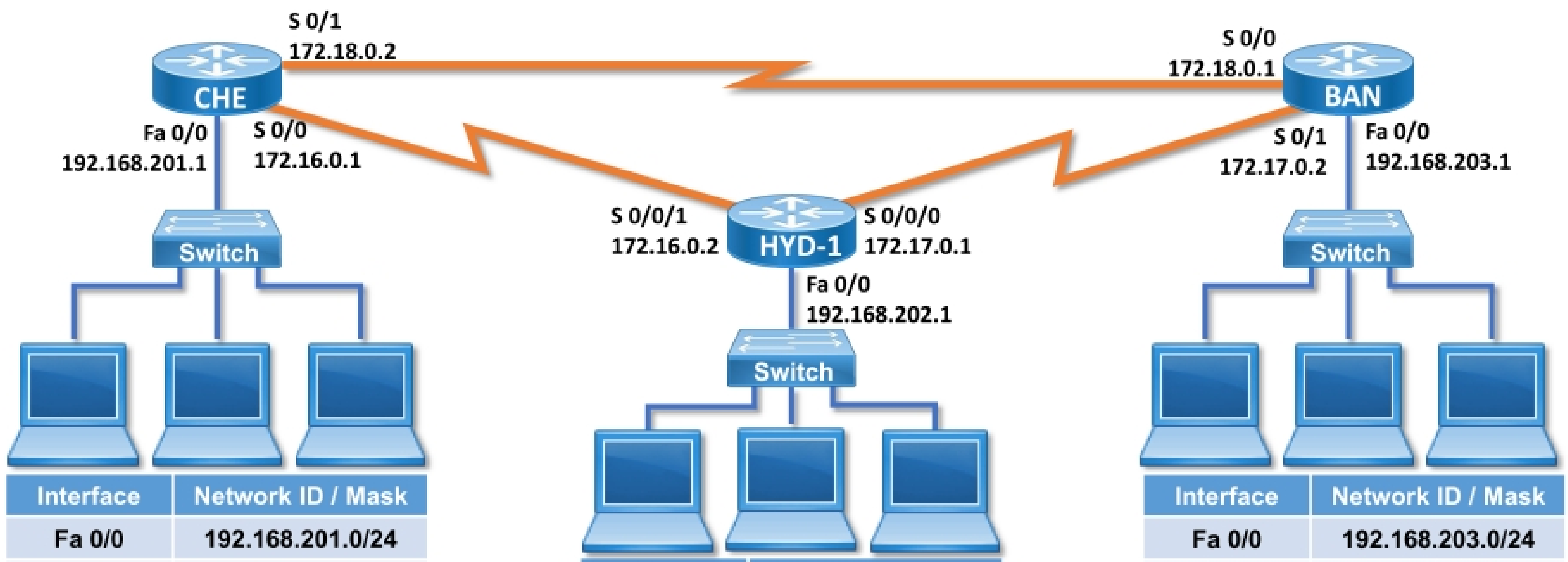


Static Routing

- Static routes are configured, maintained and updated by network administrator manually.
- Administrator should know the destination IP network for configuration.
- Administrative distance for Static Route is 1.

Administrative Distance (AD) is the "reliability" of the routing protocol. AD range is 0-255, lesser the administrative distance, higher the priority

Enabling Routing on IPv4 Network



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16
S 0/1	172.18.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	172.17.0.0/16
S 0/0/1	172.16.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	172.18.0.0/16
S 0/1	172.17.0.0/16

Enabling Routing on IPv4 Network - Configuration

Router(config) # ip routing

Enabling Routing on IPv4 Network - Configuration

ZOOM TECHNOLOGIES

CHE

CHE (config) # ip routing

BAN

BAN (config) # ip routing

HYD-1

HYD-1 (config) # ip routing

Network Diagram

CCIE CCNP CCNA

Enabling Routing on IPv4 Network - Verification

ZOOM TECHNOLOGIES

Verify the routing table

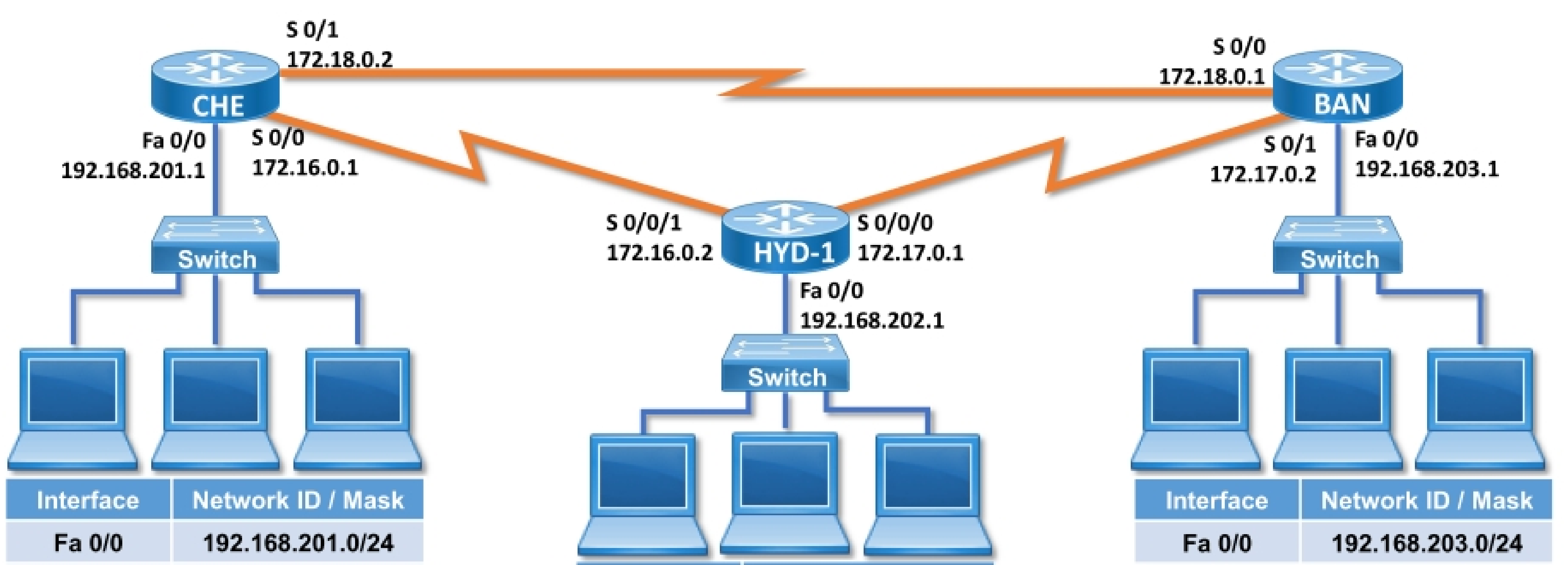
Router # show ip route

CCIE CCNP CCNA

Static Routing on IPv4 Network - Configuration

Router(config) # ip route < Destination Network ID >
< Destination Subnet Mask > < Next Hop IP address >

Static Routing on IPv4 Network



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16
S 0/1	172.18.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	172.17.0.0/16
S 0/0/1	172.16.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	172.18.0.0/16
S 0/1	172.17.0.0/16

Static Routing on IPv4 Network - Configuration

ZOOM TECHNOLOGIES

CHE

CHE (config) # ip route 192.168.202.0 255.255.255.0 172.16.0.2
CHE (config) # ip route 192.168.203.0 255.255.255.0 172.18.0.1

BAN

BAN (config) # ip route 192.168.202.0 255.255.255.0 172.17.0.1
BAN (config) # ip route 192.168.201.0 255.255.255.0 172.18.0.2

HYD-1

HYD-1 (config) # ip route 192.168.201.0 255.255.255.0 172.16.0.1
HYD-1 (config) # ip route 192.168.203.0 255.255.255.0 172.17.0.2

Network Diagram

CCIE CCNP CCNA

Static Routing on IPv4 Network - Verification

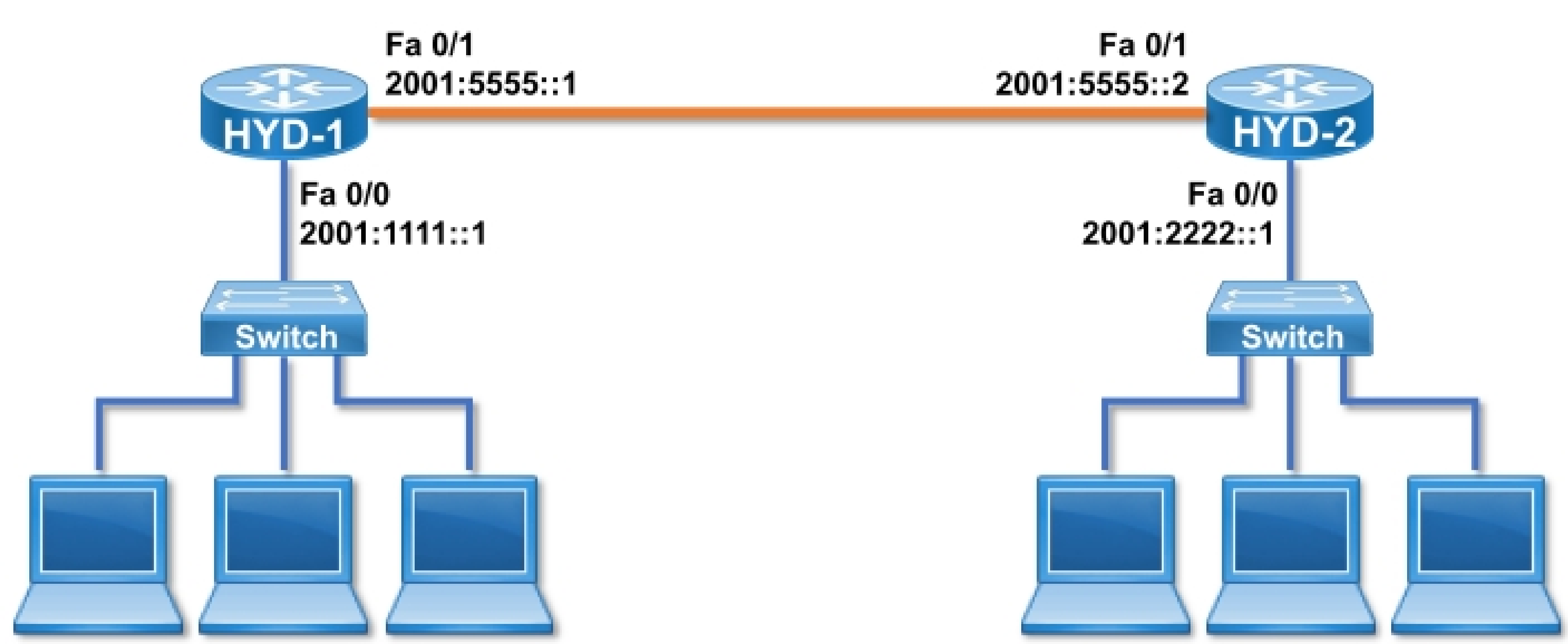
ZOOM TECHNOLOGIES

Verify the routing table

Router # show ip route

CCIE CCNP CCNA

Enabling Routing on IPv6 Network



Interface	Network ID / Mask
Fa 0/0	2001:1111::/64
Fa 0/1	2001:5555::/64

Interface	Network ID / Mask
Fa 0/0	2001:2222::/64
Fa 0/1	2001:5555::/64

Enabling Routing on IPv6 Network - Configuration

Router(config) # ipv6 unicast-routing

Enabling Routing on IPv6 Network - Configuration

HYD-1

HYD-1 (config) # ipv6 unicast-routing

HYD-2

HYD-2 (config) # ipv6 unicast-routing

Network Diagram

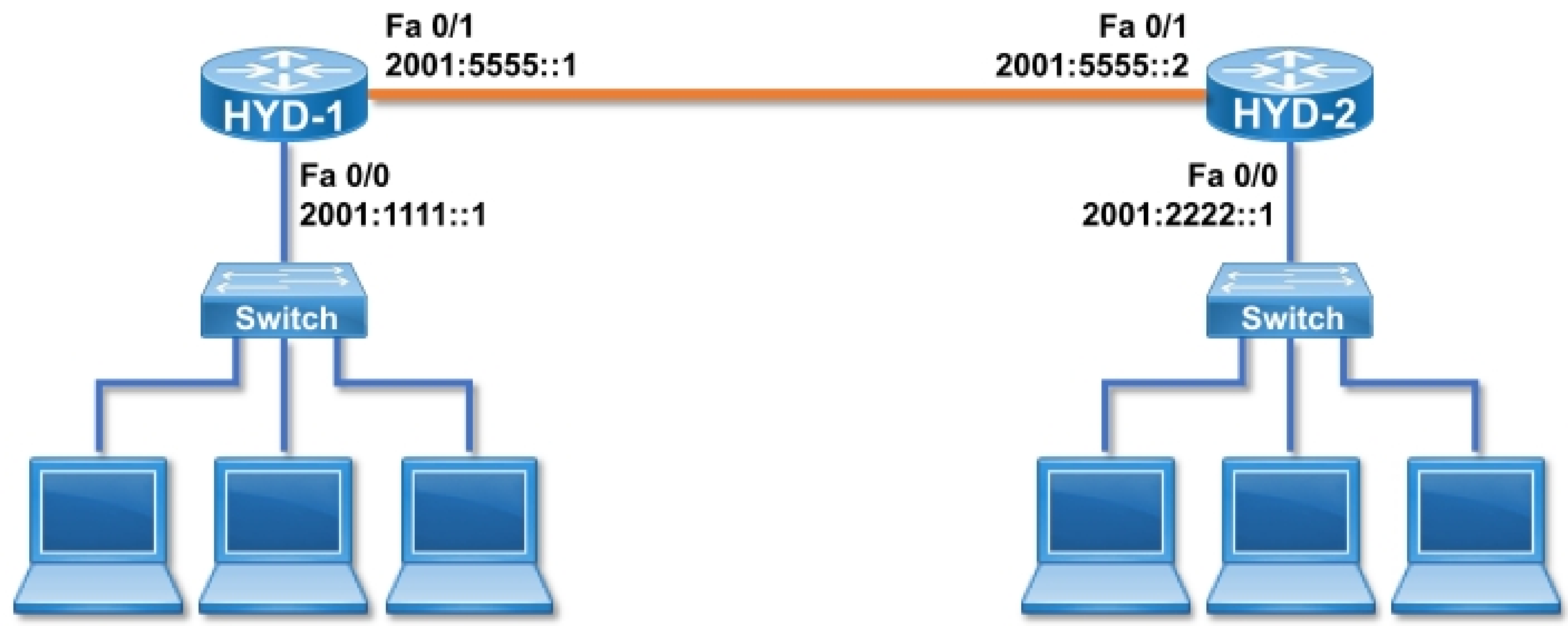
Enabling Routing on IPv6 Network - Verification

Router # show ipv6 route

Static Routing on IPv6 Network - Configuration

Router(config) # ipv6 route < ipv6 Destination prefix/prefix-length>
< Next Hop IP address >

Static Routing on IPv6 Network



Interface	Network ID / Mask
Fa 0/0	2001:1111::/64
Fa 0/1	2001:5555::/64

Interface	Network ID / Mask
Fa 0/0	2001:2222::/64
Fa 0/1	2001:5555::/64

Static Routing on IPv6 Network - Configuration

HYD-1

HYD-1 (config) # ipv6 route 2001:2222::/64 2001:5555::2

HYD-2

HYD-2 (config) # ipv6 route 2001:1111::/64 2001:5555::1

Network Diagram

Static Routing on IPv6 Network - Verification

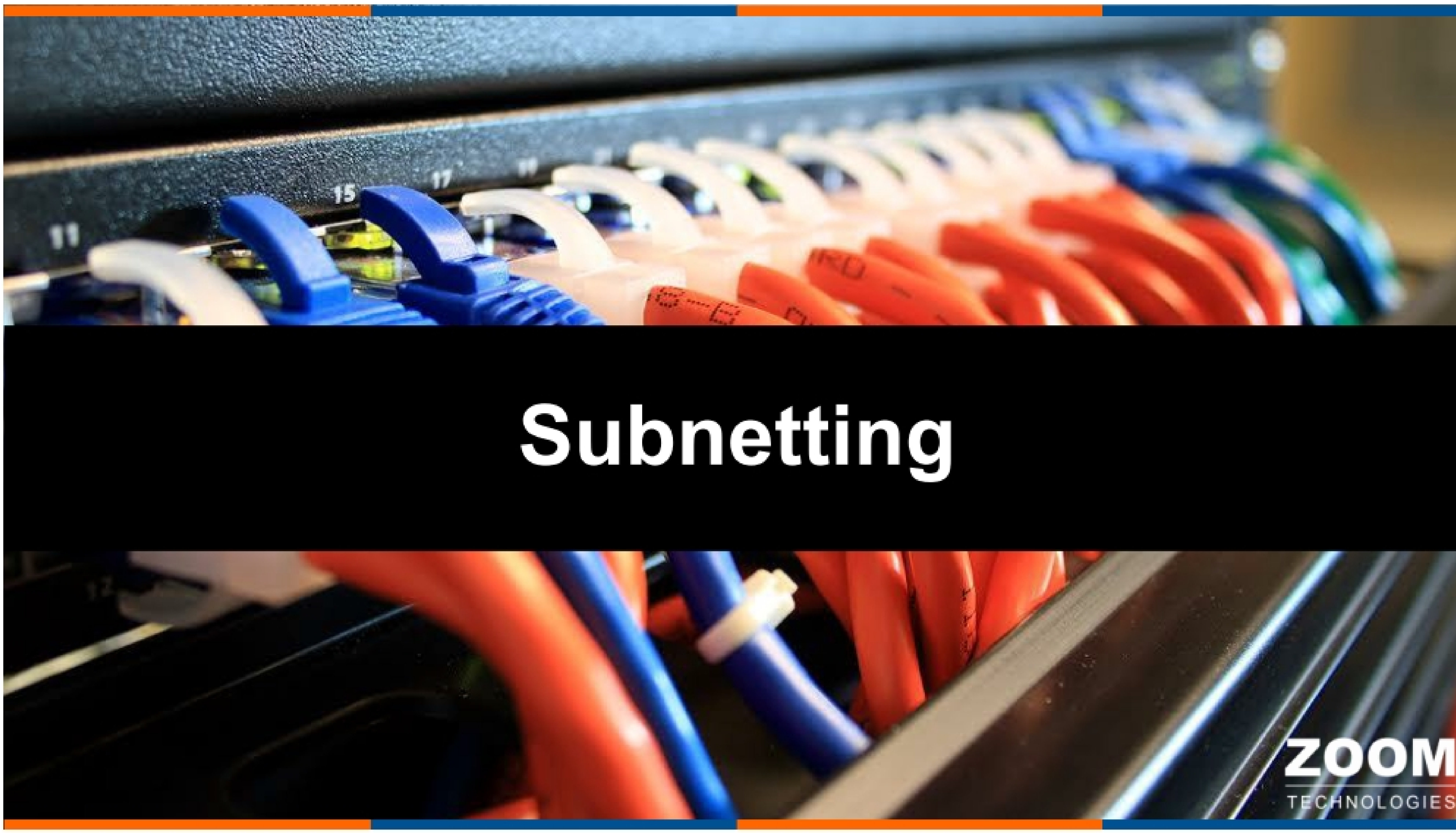
Verify the routing table

Router # show ipv6 route

Network Diagram

Advantages and Disadvantages of Static routing

Advantages	Disadvantages
Secured	No Automatic Updates
Reliable	Need of Destination network ID for the configuration
Faster	Administrative work is more
No wastage of bandwidth	Used in Small networks



Subnetting

- Creating Multiple independent Networks from a single Network
- Converting Host bits into Network bits (i.e. converting 0's into 1's)
- Subnetting can be performed in two ways
  - FLSM (Fixed Length Subnet Mask)
  - VLSM (Variable Length Subnet Mask)
- Subnetting can be done based on requirement
  - Number of Networks Required?
  - Number of Hosts Required?
  - Cisco Slash Notation

Note:-

It is very useful for Internet Service Providers (ISP), Large Organizations/ Companies etc.,

Requirement of Networks

- A corporate network has 200 PC's
- Which class of IP Address is preferred for the network ?

  Answer : Class C
- There are 4 departments with 50 pc's each

  Marketing → 192.168.1.1 to 192.168.1.50

  Sales → 192.168.1.51 to 192.168.1.100

  Finance → 192.168.1.101 to 192.168.1.150

  IT → 192.168.1.151 to 192.168.1.200

Administrators Requirement

- Inter-department communication should not be there

Solution :

- Allocate different Networks to each Department

i.e.,

Marketing → 192.168.1.1 to 192.168.1.50

Sales → 192.168.2.1 to 192.168.2.50

Finance → 192.168.3.1 to 192.168.3.50

IT → 192.168.4.1 to 192.168.4.50

Main Aim of Subnetting

- Problem with the previous scenario is
  - Wastage of IP addresses, if it is Public IP addresses (Approx. 800)
  - To reduce the wastage of IP addresses, we have Subnetting

Power table

POWER TABLE			
$2^1 = 2$	$2^9 = 512$	$2^{17} = 131072$	$2^{25} = 33554432$
$2^2 = 4$	$2^{10} = 1024$	$2^{18} = 262144$	$2^{26} = 67108864$
$2^3 = 8$	$2^{11} = 2048$	$2^{19} = 524288$	$2^{27} = 134217728$
$2^4 = 16$	$2^{12} = 4096$	$2^{20} = 1048576$	$2^{28} = 268435456$
$2^5 = 32$	$2^{13} = 8192$	$2^{21} = 2097152$	$2^{29} = 536870912$
$2^6 = 64$	$2^{14} = 16384$	$2^{22} = 4194304$	$2^{30} = 1073741824$
$2^7 = 128$	$2^{15} = 32768$	$2^{23} = 8388608$	$2^{31} = 2147483648$
$2^8 = 256$	$2^{16} = 65536$	$2^{24} = 16777216$	$2^{32} = 4294967296$

Some Important Values

VALUES IN SUBNET MASK		
Bit	Value	Mask
1	128	10000000
2	192	11000000
3	224	11100000
4	240	11110000
5	248	11111000
6	252	11111100
7	254	11111110
8	255	11111111

Requirement of Subnets – 4 no's ?

- Class C : 192.168.1.0
- Octet Format is N . N . N . H
  Network bits : 24 Host bits : 8
- Subnets required : 4 no's
  - = $2^n \geq$ Req. of Subnet
  - = $2^n \geq 4$
  - = $2^2 \geq 4$
  - = 4 subnets
- No. of Hosts / Subnet
  - = $2^{\text{no of host bits}}$ -2
  - = $2^6 - 2$ (-2 is for Network ID & Broadcast ID)
  - = 64 - 2
  - = 62 Hosts / Subnet

Continued...

- **Customized subnet mask**

255.	255.	255.	0	=	255.	255.	255.	192
11111111.	11111111.	11111111.	00000000	=	11111111.	11111111.	11111111.	11000000

- **Subnet Range**

Network ID		Broadcast ID
192.168.1.0	-	192.168.1.63
192.168.1.64	-	192.168.1.127
192.168.1.128	-	192.168.1.191
192.168.1.192	-	192.168.1.255

Requirement of Subnets – 30 no's ?

- **Class C : 192.168.1.0**
- **Octet Format is N . N . N . H**

  Network bits : 24 **Host bits : 8**
- **Subnets required : 32 no's**

  = $2^n \geq$ Req. of Subnet

  = $2^n \geq 4$

  = $2^5 \geq 4$

  = 32 subnets
- **No. of Hosts / Subnet**

  = $2^{\text{no of host bits}} - 2$

  = $2^3 - 2$ (-2 is for Network ID & Broadcast ID)

  = 8 - 2

  = 6 Hosts / Subnet

Continued…

- Customized subnet mask

$$\underbrace{255.}_{11111111.}\ \underbrace{255.}_{11111111.}\ \underbrace{255.}_{11111111.}\ \underbrace{0}_{00000000} = \underbrace{255.}_{11111111.}\ \underbrace{255.}_{11111111.}\ \underbrace{255.}_{11111111.}\ \underbrace{248}_{11111000}$$

- Subnet Range

Network ID		Broadcast ID
192.168.1.0	-	192.168.1.7
192.168.1.8	-	192.168.1.15
192.168.1.16	-	192.168.1.23
192.168.1.248	-	192.168.1.255

Requirement of Host – 12 no's ?

- Class C : 192.168.1.0
- Octet Format is N . N . N . H

  Network bits : 24 Host bits : 8
- Host required : 12 no's

  = $2^n - 2 \geq$ Req. of Host (-2 is for Network ID & Broadcast ID)

  = $2^4 - 2 \geq 12$

  = 16 - 2

  = 14 Hosts
- No. of Subnets

  = $2^{\text{no of network bits}}$

  = 2^4

  = 16 subnets

Continued…

- **Customized subnet mask**

$$\overbrace{11111111}^{255}.\overbrace{11111111}^{255}.\overbrace{11111111}^{255}.\overbrace{00000000}^{0} = \overbrace{11111111}^{255}.\overbrace{11111111}^{255}.\overbrace{11111111}^{255}.\overbrace{11110000}^{240}$$

- **Subnet Range**

Network ID		Broadcast ID
192.168.1.0	-	192.168.1.15
192.168.1.16	-	192.168.1.31
192.168.1.32	-	192.168.1.47
192.168.1.240	-	192.168.1.255

Requirement of Host – 2 no's ?

- **Class C : 192.168.1.0**
- **Octet Format is N . N . N . H**

  Network bits : 24 **Host bits : 8**
- **Host required : 2 no's**

  = $2^n - 2 \geq$ Req. of Host (-2 is for Network ID & Broadcast ID)

  = $2^2 - 2 \geq 2$

  = $4 - 2$

  = 2 Hosts
- **No. of Subnets**

  = $2^{\text{no of network bits}}$

  = 2^6

  = 64 subnets

Continued...

- **Customized subnet mask**

$$\underbrace{11111111}_{255.}.\underbrace{11111111}_{255.}.\underbrace{11111111}_{255.}.\underbrace{00000000}_{0} = \underbrace{11111111}_{255.}.\underbrace{11111111}_{255.}.\underbrace{11111111}_{255.}.\underbrace{11111100}_{252}$$

- **Subnet Range**

Network ID		Broadcast ID
192.168.1.0	-	192.168.1.3
192.168.1.4	-	192.168.1.7
192.168.1.8	-	192.168.1.11
192.168.1.252	-	192.168.1.255

Cisco Slash Notation – example-1

- **Class C : 192.168.1.65/25**

  Network bits : 25 **Host bits : 7**

- **No. of Subnets**

  = $2^{\text{no of network bits}}$

  = 2^1

  = 2 subnets

- **No. of Hosts / Subnet**

  = $2^{\text{no of host bits}} - 2$

  = $2^7 - 2$ (-2 is for Network ID & Broadcast ID)

  = 128 - 2

  = 126 Hosts / Subnet

Continued…

- Customized subnet mask

$$\underbrace{255.}_{11111111.}\ \underbrace{255.}_{11111111.}\ \underbrace{255.}_{11111111.}\ \underbrace{0}_{00000000} = \underbrace{255.}_{11111111.}\ \underbrace{255.}_{11111111.}\ \underbrace{255.}_{11111111.}\ \underbrace{128}_{10000000}$$

- Subnet Range

Network ID		Broadcast ID
192.168.1.0	-	192.168.1.127
192.168.1.128	-	192.168.1.255

Cisco Slash Notation – example-2

- Class C : 192.168.1.65/27

  Network bits : 27 Host bits : 5
- No. of Subnets

  = $2^{\text{no of network bits}}$

  = 2^3

  = 8 subnets
- No. of Hosts / Subnet

  = $2^{\text{no of host bits}}$ -2

  = 2^5 – 2 (-2 is for Network ID & Broadcast ID)

  = 32 - 2

  = 30 Hosts / Subnet

Continued...

- **Customized subnet mask**

255. 255. 255. 0 = 255. 255. 255. 224

11111111. 11111111. 11111111. 00000000 = 11111111. 11111111. 11111111. 11100000

- **Subnet Range**

Network ID		Broadcast ID
192.168.1.0	-	192.168.1.31
192.168.1.32	-	192.168.1.63
192.168.1.64	-	192.168.1.95
192.168.1.224	-	192.168.1.255

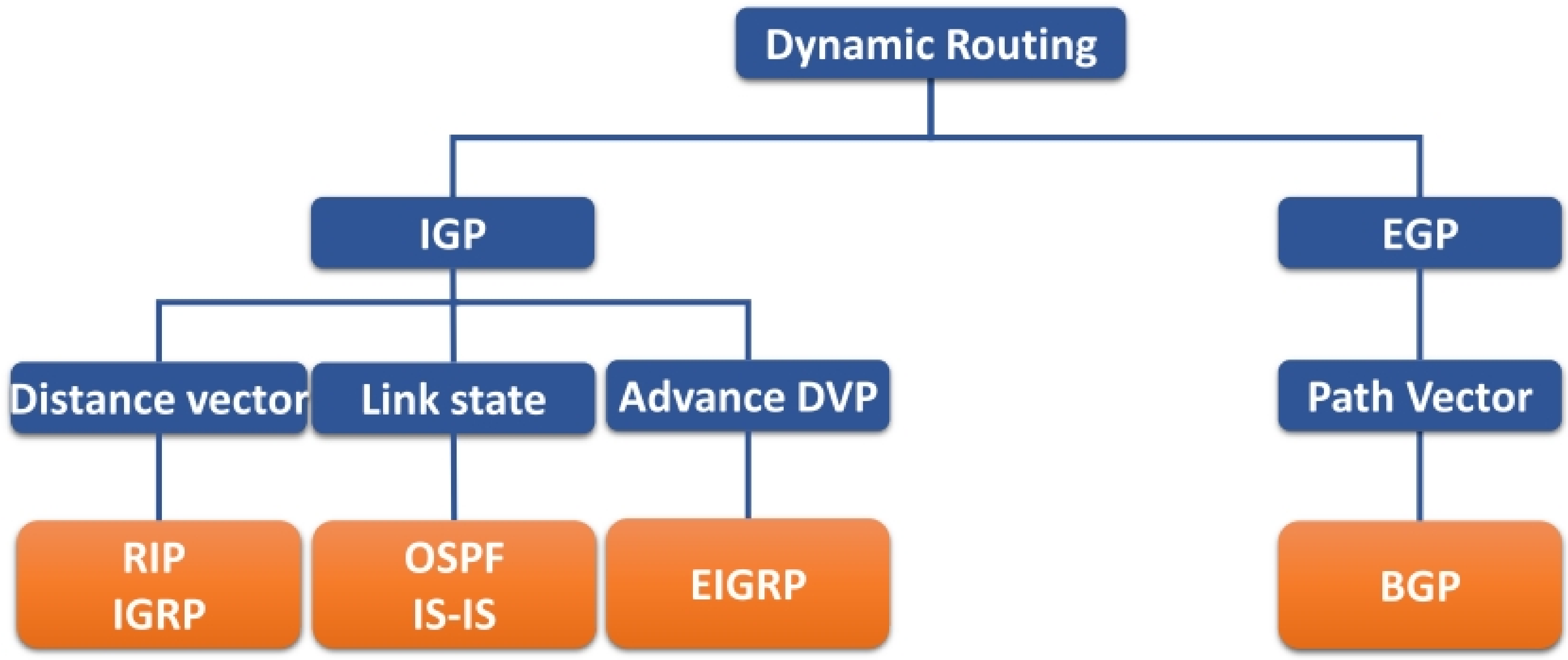
Overview of Routing Protocol

- Purpose of Routing Protocol includes the following functions:
  - Discover the neighbor, finding the best paths
  - Maintaining the up to date routing information
  - Choosing the best path in available paths.
  - Whenever the best path is going down finding the new path and forwarding the data through that path.

Advantages of Dynamic Routing

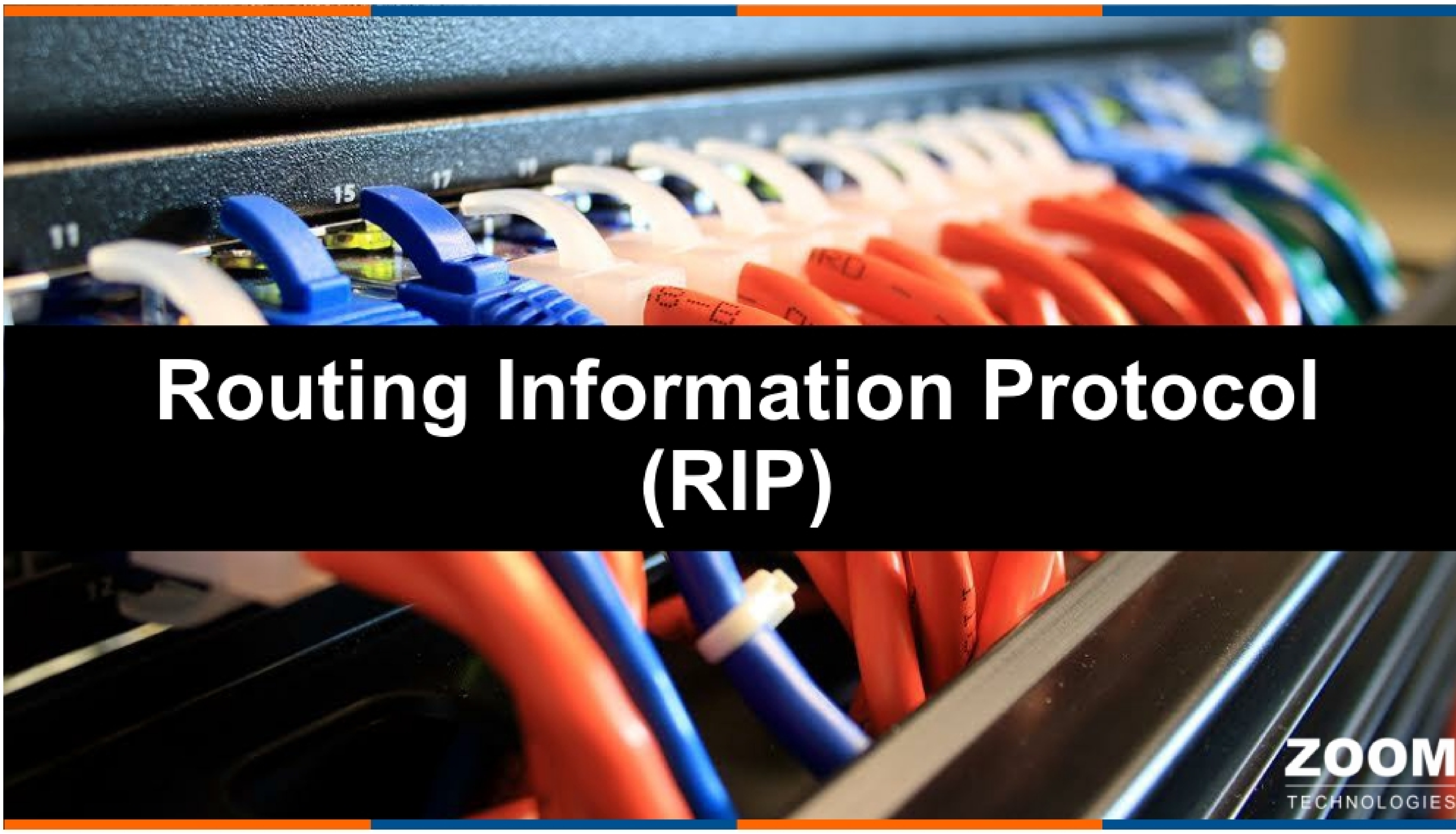
- Automatic updates.
- Changes in the network topology are updated dynamically
- Only the directly connected network information is required for the configuration
- Less Administrative work
- Selecting the best path to destination networks
- Finding the second best path if best path is no longer available.
- More scalable
- Used for medium and large Networks

Types of Dynamic Routing Protocols



Classfull v/s Classless Routing Protocol

Classfull Routing Protocol	Classless Routing Protocol
• Do not send the subnet mask in the update	• Carries the subnet mask in the update
• Doesn't support subnetting	• Supports subnetting
• Ex: RIP v1, IGRP	• Ex: RIP v2, EIGRP, OSPF



RIP Characteristics

- Distance Vector Protocol
- Open standard
- Uses Bellman Ford Algorithm
- Classless routing protocol
- Metric = Hop Count
- Maximum hop count is 15.
- Updates are sent through the multicast address 224.0.0.9
- RIP sends periodic updates for every 30 seconds.
- RIP supports equal cost load balancing by default 4 paths (maximum upto 16 paths)

RIP Characteristics

- Complete routing table is sent as update
- Each update can contain maximum of 25 routes
- Administrative distance is 120
- Uses the UDP port no 520
- Also known as “Routing by Rumor”

Loopback Interface

- A loopback interface is a virtual interface that resides on a router.
- Loopback interfaces are very useful because they will never go down, unless the entire router goes down.
- By default, router doesn’t have any loopback interfaces (loopback interfaces are not enabled by default), but they can easily be created.

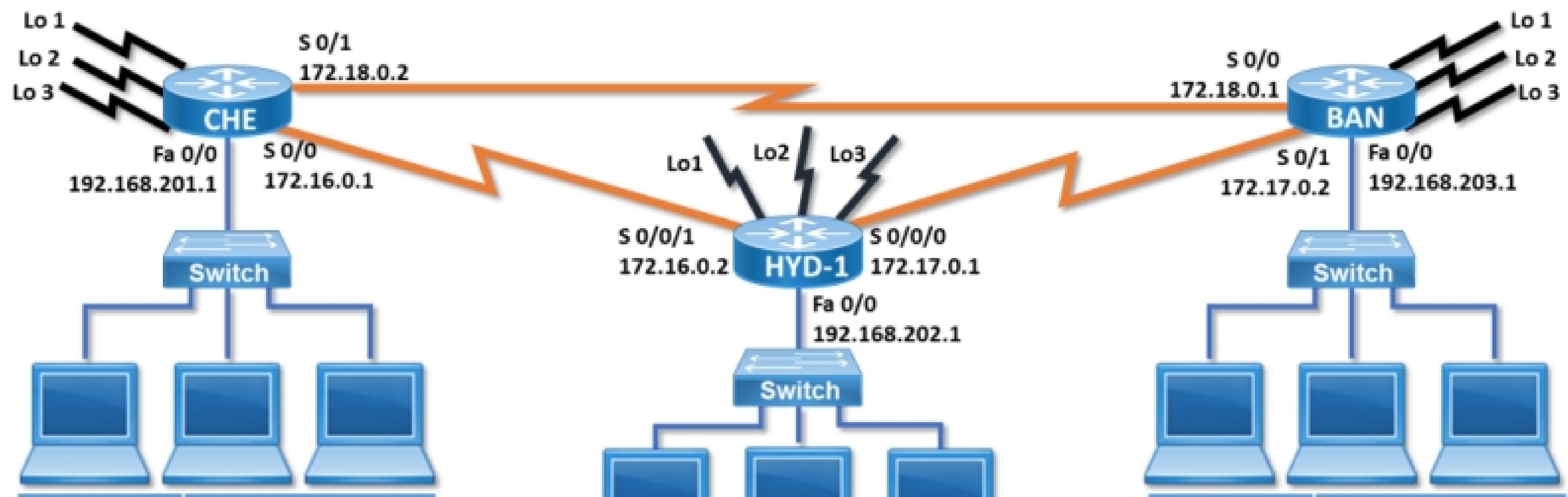
Loopback Interface - Configuration

```
Router (config) #  interface  loopback  < interface no. >
Router (config-if) #  ip address < ip address > < subnet mask >
Router (config-if) #  end
```

RIP on IPv4 Network - Configuration

```
Router(config) #  ip routing
Router(config) #  router rip
Router(config-router) #  version 2
Router(config-router) #  network < Network ID >
```

RIP on IPv4 Network



CHE

Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16
S 0/1	172.18.0.0/16

Interface	IP Address / Mask
Lo1	16.1.1.1/24
Lo2	16.1.2.1/24
Lo3	16.1.3.1/24

HYD-1

Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	172.17.0.0/16
S 0/0/1	172.16.0.0/16

Interface	IP Address / Mask
Lo1	17.1.1.1/24
Lo2	17.1.2.1/24
Lo3	17.1.3.1/24

BAN

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	172.18.0.0/16
S 0/1	172.17.0.0/16

Interface	IP Address / Mask
Lo1	18.1.1.1/24
Lo2	18.1.2.1/24
Lo3	18.1.3.1/24

RIP on IPv4 Network - Configuration

CHE

```
CHE (config) # ip routing
CHE (config) # router rip
CHE (config-router) # version 2
CHE (config-router) # network 192.168.201.0
CHE (config-router) # network 172.16.0.0
CHE (config-router) # network 172.18.0.0
CHE (config-router) # network 16.0.0.0
CHE (config-router) # end
CHE #
```

BAN

```
BAN (config) # ip routing
BAN (config) # router rip
BAN (config-router) # version 2
BAN (config-router) # network 192.168.203.0
BAN (config-router) # network 172.17.0.0
BAN (config-router) # network 172.18.0.0
BAN (config-router) # network 18.0.0.0
BAN (config-router) # end
BAN #
```

HYD-1

```
HYD-1 (config) # ip routing
HYD-1 (config) # router rip
HYD-1 (config-router) # version 2
HYD-1 (config-router) # network 192.168.202.0
HYD-1 (config-router) # network 172.16.0.0
HYD-1 (config-router) # network 172.17.0.0
HYD-1 (config-router) # network 17.0.0.0
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

RIP on IPv4 Network - Verification

Verify the routing table

Router # show ip route

To verify the protocols

Router # show ip protocols

RIP Timers

- Update Timer : 30 sec
  - Time between two consecutive updates
- Invalid Timer : 180 sec
  - Time a router waits to hear an update from the neighbor
  - The route is marked as unreachable if there is no update for this time period
- Flush Timer : 240 sec
  - Time after which the invalid route is removed from the routing table

RIP Updates

To verify the RIP Timers

Router # show ip protocols

Verify RIP Update Packets

Router # terminal monitor

Router # debug ip rip

Change RIP Timers

Router (config) # router rip

Router (config-router) # timers basic <update timer> <invalid timer> <holddown time> <flush timer>


```
HYD-1 (config) # router rip
HYD-1 (config-router) # timers basic 15 30 90 90
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

Passive interface

- **Passive interface is configured to stop the updates to exit out of the interface.**
- **If passive interface is configured between the routers no updates will be exchanged.**

Configure Passive interface

Router(config) # router rip

Router(config-router) # passive-interface <interface type> <no.>


```
HYD-1 (config) # router rip
HYD-1 (config-router) #  passive-interface FastEthernet0/0
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

Summarization

- Combining the continuous networks in one full network and advertising to neighbor router is called as summarization.
- Advantages of Summarization
  - Less number of updates
  - Reducing the size of routing table

Disable auto-summary

```
Router(config) #  router rip
Router(config-router) # no auto-summary
Router(config-router)# exit
```

HYD-1

```
HYD-1 (config) # router rip
HYD-1 (config-router) #  no auto-summary
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

RIPng Characteristics

ZOOM TECHNOLOGIES

- **RFC 2080 - RIP for ipv6**
- **Uses the multicast group FF02::9**
- **Multiple instances can be created on one router which is not possible in RIP IPv4.**

CCIE CCNP CCNA

RIPng on IPv6 Network - Configuration

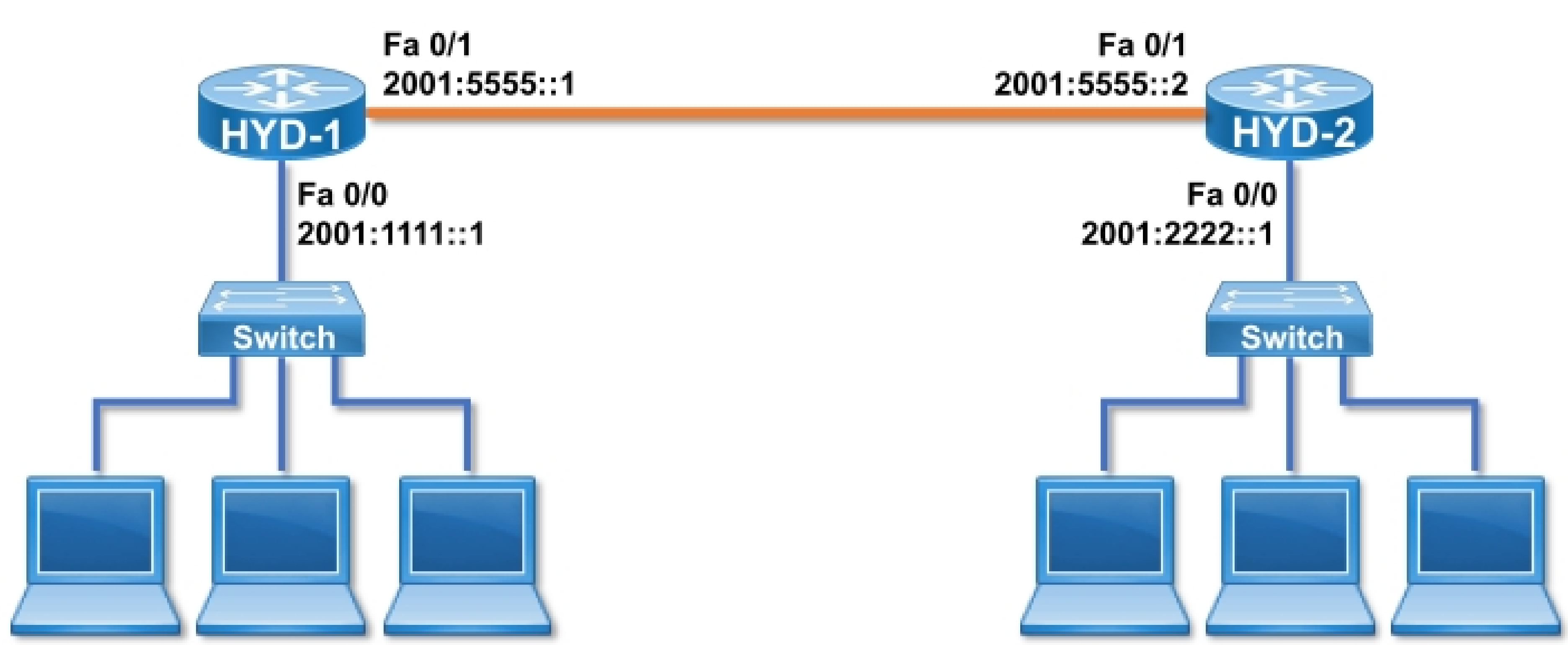
Router(config) # ipv6 unicast-routing

Router(config) # ipv6 router rip <name>

Router(config) # interface < interface type > < no. >

Router(config-if) # ipv6 rip <name> enable

RIPng on IPv6 Network



Interface	Network ID / Mask
Fa 0/0	2001:1111::/64
Fa 0/1	2001:5555::/64

Interface	Network ID / Mask
Fa 0/0	2001:2222::/64
Fa 0/1	2001:5555::/64

RIPng on IPv6 Network - Configuration

ZOOM TECHNOLOGIES

HYD-1

```
HYD-1 (config) # ipv6 unicast-routing
HYD-1 (config) # ipv6 router rip cisco
HYD-1 (config-rtr) # exit
HYD-1 (config) # interface fastethernet 0/0
HYD-1 (config-if) # ipv6 rip cisco enable
HYD-1 (config-if) # exit
HYD-1 (config) # interface fastethernet 0/1
HYD-1 (config-if) # ipv6 rip cisco enable
HYD-1 (config-if) # end
HYD-1 #
```

HYD-2

```
HYD-2 (config) # ipv6 unicast-routing
HYD-2 (config) # ipv6 router rip cisco
HYD-2 (config-rtr) # exit
HYD-2 (config) # interface fastethernet 0/0
HYD-2 (config-if) # ipv6 rip cisco enable
HYD-2 (config-if) # exit
HYD-2 (config) # interface fastethernet 0/1
HYD-2 (config-if) # ipv6 rip cisco enable
HYD-2 (config-if) # end
HYD-2 #
```

Network Diagram

CCIE CCNP CCNA

RIPng on IPv6 Network - Verification

ZOOM TECHNOLOGIES

Verify the routing table

Router # show ipv6 route

Network Diagram

CCIE CCNP CCNA

Disadvantages of RIP

- More Bandwidth is utilized for sending the updates.
- Does not consider the bandwidth in metric calculations, uses only hop count
- Slow convergence

Link State Routing Protocol

- Every router maintains the full picture of the topology
- Link state protocol is more scalable
- Any change in the topology is quickly updated.
- Link state protocol has more advantages compared to distance vector routing protocol

OSPF Characteristics

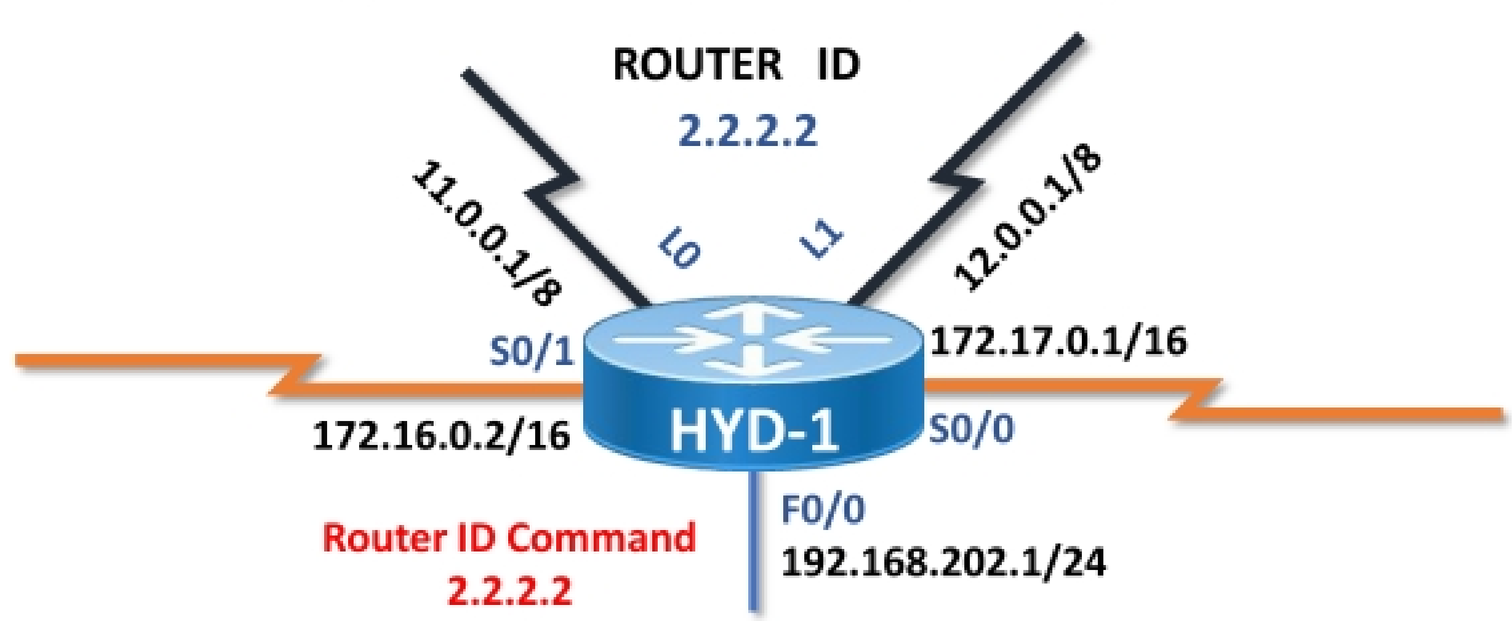
- Link State Protocol
- Open standard
- Uses Dijkstra (Shortest Path First – SPF) Algorithm
- Classless routing protocol
- Metric = cost= 10^8 / Bandwidth in bps (CISCO)
- Updates are sent through Multicast IP address 224.0.0.5
- OSPF protocol supports equal cost load balancing
  - Supports Default 4 paths maximum of 16 paths.
- Administrative distance is 110

OSPF Characteristics

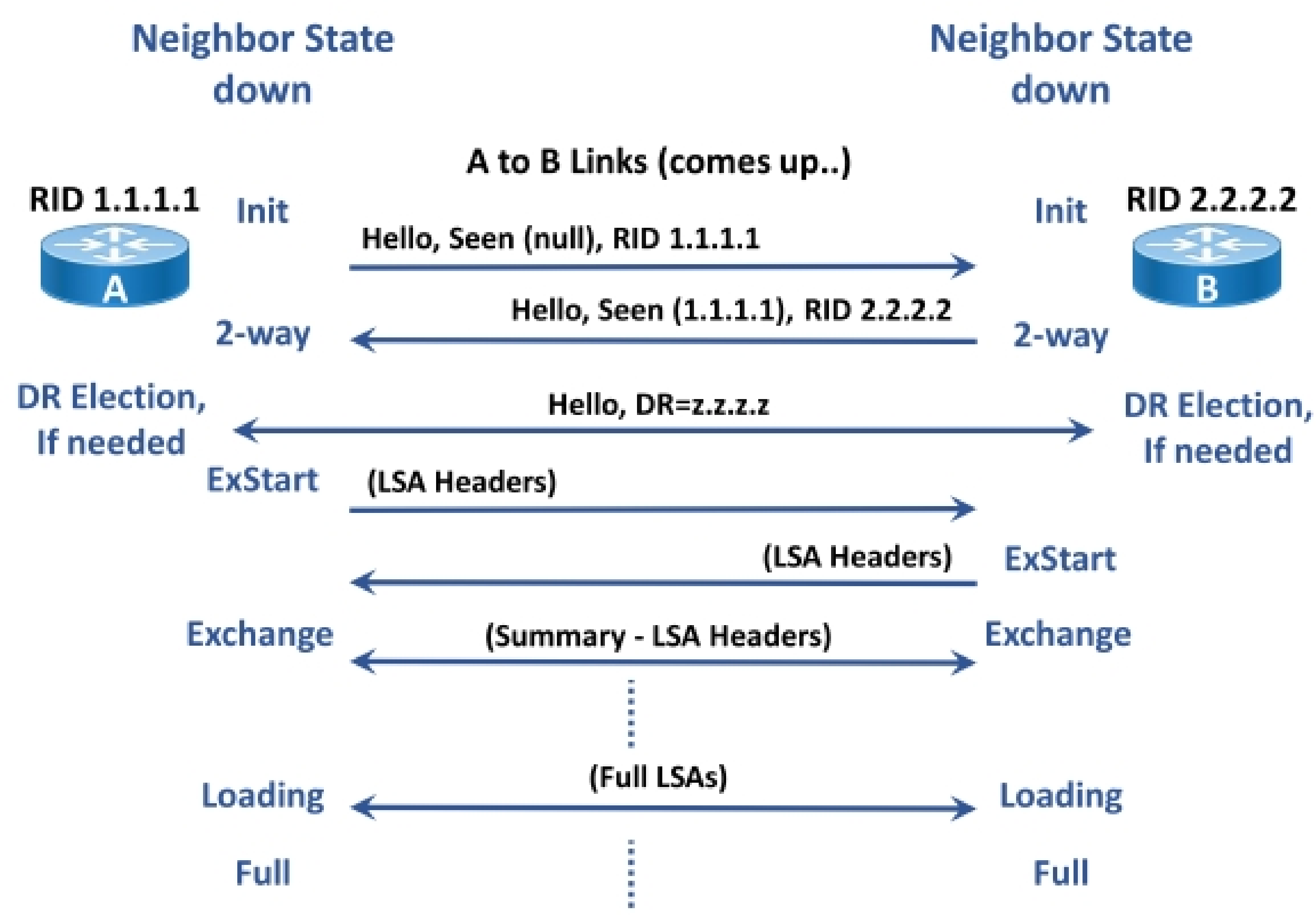
- Neighbor is discovered and established by hello packets
- Hello packets 10 seconds, Dead interval 40 seconds.
- Unlimited Hop Count.
- OSPF sends updates (LSAs) when there is a change to one of its links.
- OSPF protocol number 89.

Router ID

- The router-id is used to identify the router in OSPF
  - First preference is given to router-id command
  - Second preference is given to highest loopback interfaces configured on router
  - Third preference is given to highest physical ip address



OSPF Neighbor States



OSPF Terminology

- **Neighbor**
  - **Routers that share a common link become neighbors.**
  - **Neighbors are discovered by Hello Packets.**
  - **To become neighbors the following should match**
    - **Area ID**
    - **Network ID and Subnet Mask**
    - **Hello and Dead Intervals**
    - **Authentication (optional)**

- **Adjacencies**
  - **Adjacencies are formed once neighbor relation is established.**
  - **In Adjacencies the database details are exchanged.**

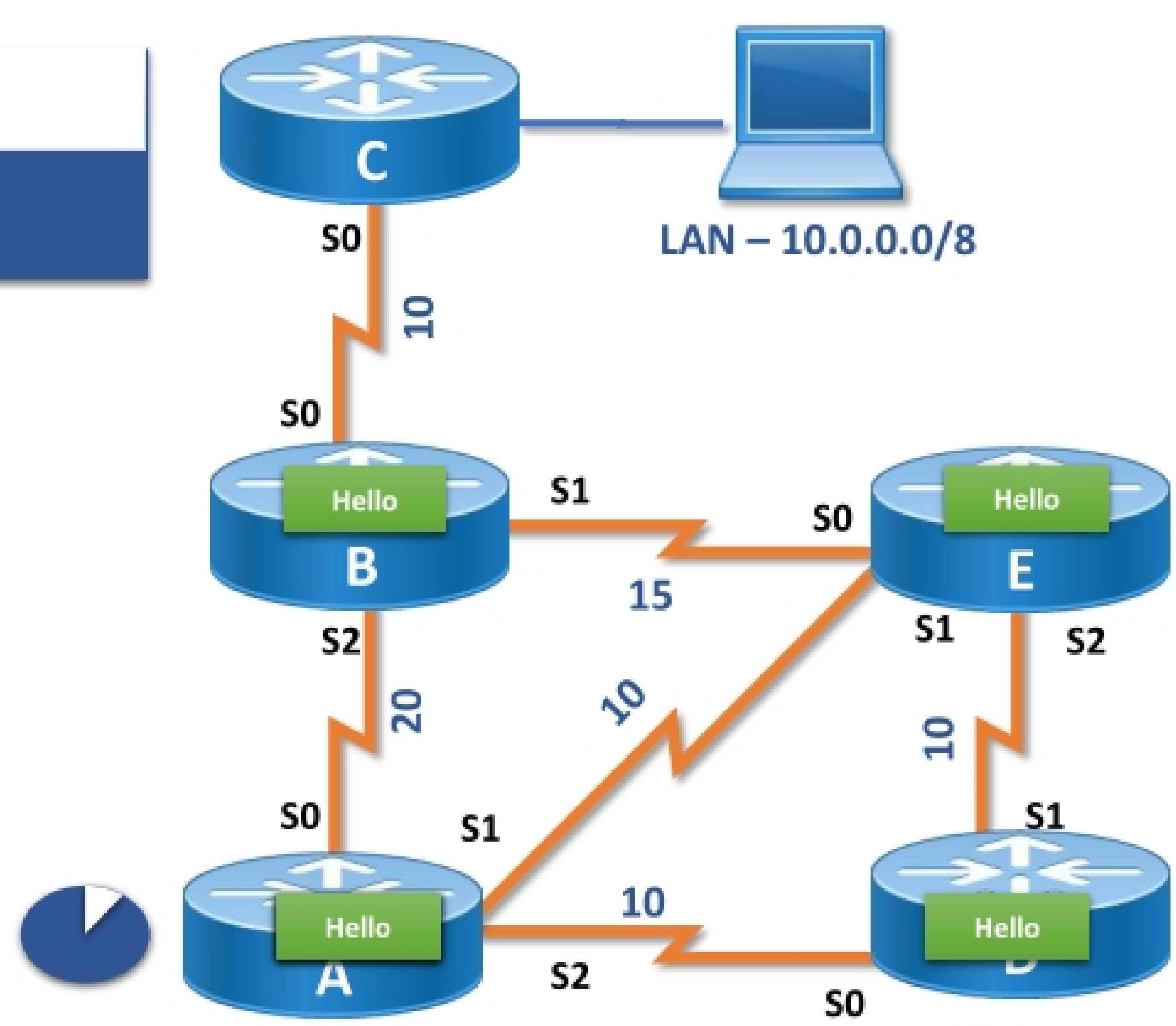
OSPF Tables

- It maintains three tables :
- Neighbor Table
  - Neighbor table contains information about the directly connected OSPF neighbors forming adjacency.
- Database Table
  - Database table contains information about the entire view of the topology with respect to each router.
- Routing Table
  - Routing table contains information about the best path calculated by the shortest path first algorithm in the database table.

OSPF - Neighbor Table

NEIGHBOR TABLE (Router A)

Neighbor	Interface
B	S0
D	S2
E	S1



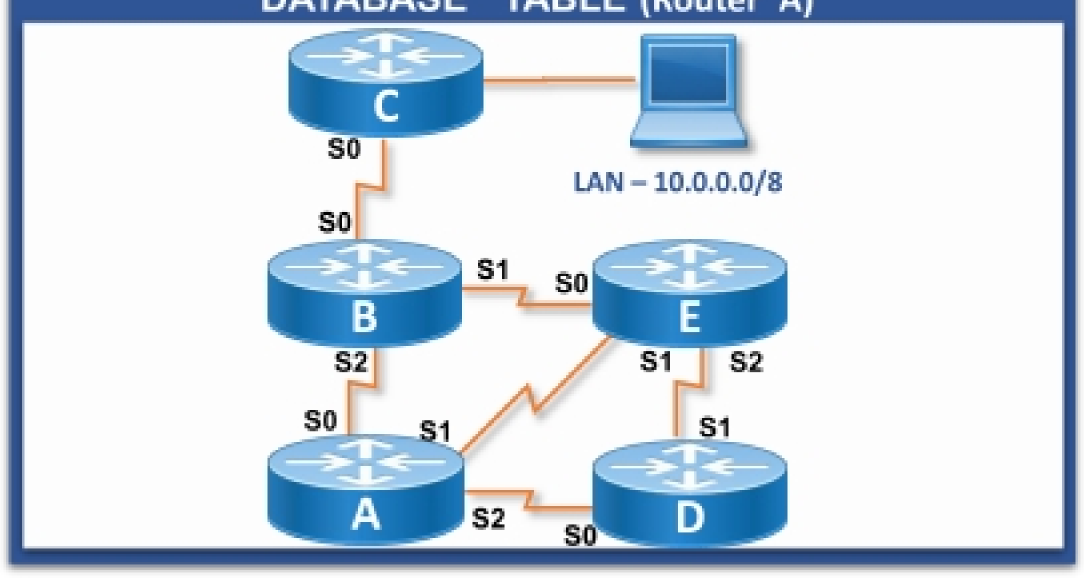
OSPF - Database Table

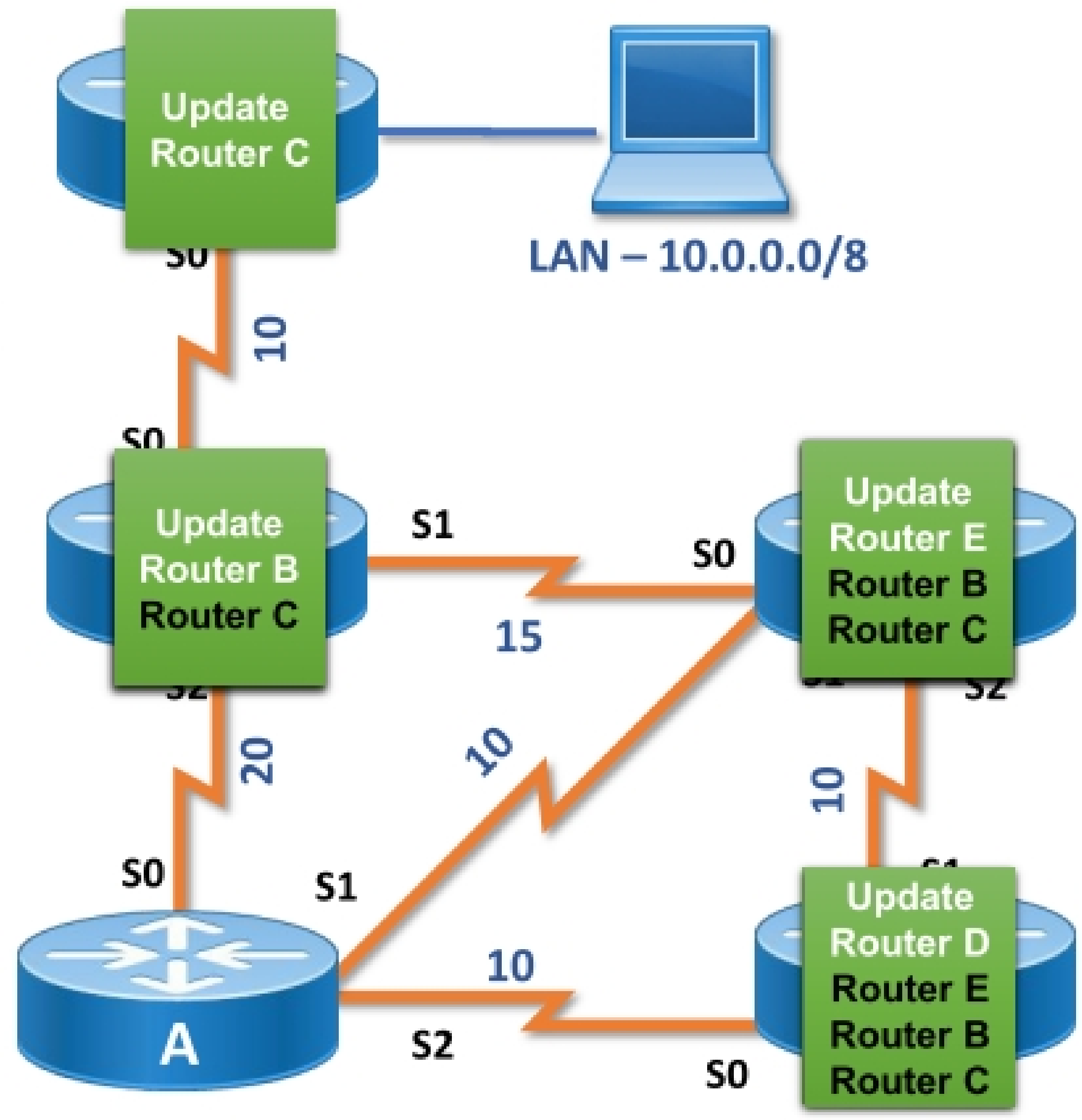
ZOOM TECHNOLOGIES

NEIGHBOR TABLE (Router A)

Neighbor	Interface
B	S0
D	S2
E	S1

DATABASE TABLE (Router A)





CCIE CCNP CCNA

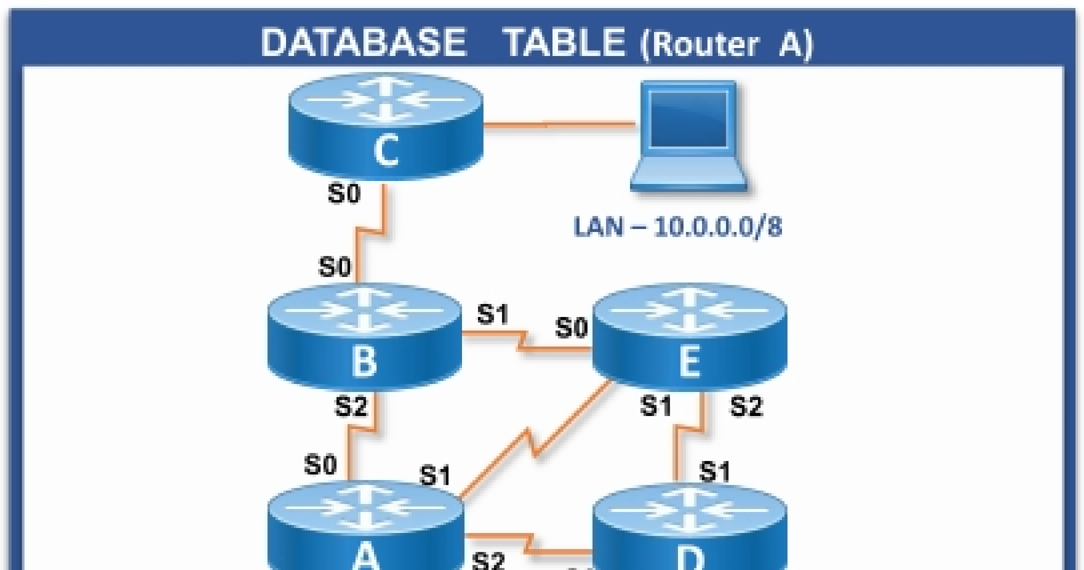
OSPF - Database Table

ZOOM TECHNOLOGIES

NEIGHBOR TABLE (Router A)

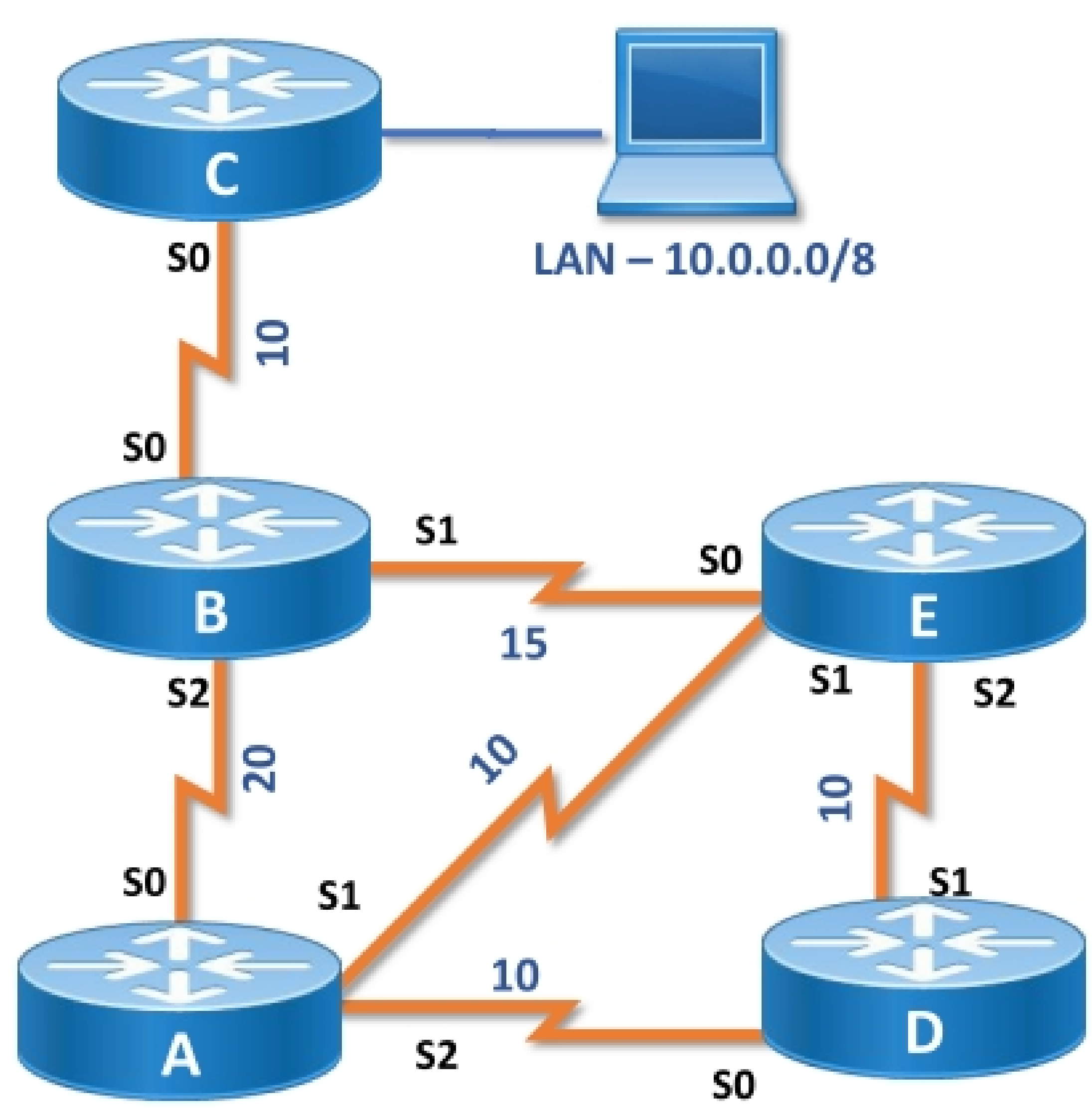
Neighbor	Interface
B	S0
D	S2
E	S1

DATABASE TABLE (Router A)



ROUTING TABLE (Router A)

O 10.0.0.0/8 [110/30] via B, 01:36, Serial0



CCIE CCNP CCNA

Wild Card Mask

- A wild card mask can be calculated using the formula :

  Global Subnet Mask
  – Subnet Mask

  Wild Card Mask

E.g.

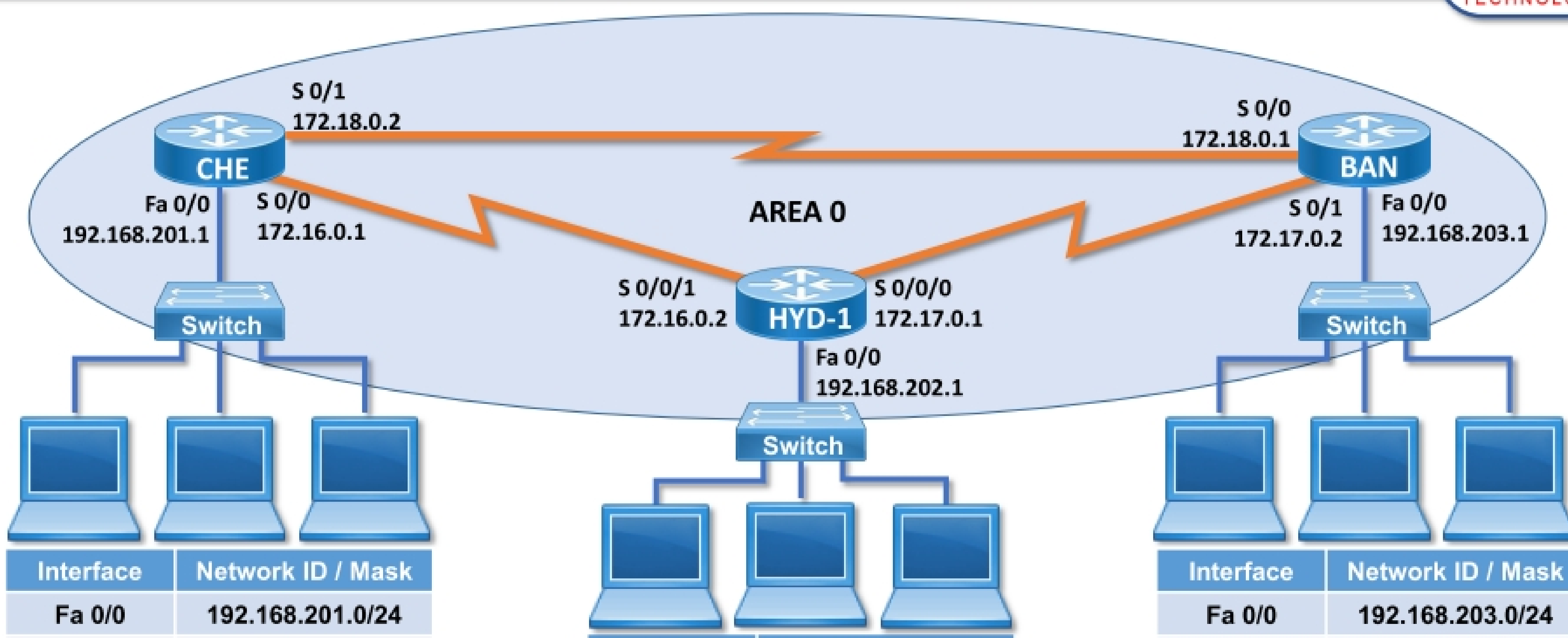
```
      255.255.255.255          255.255.255.255
–     255.255.255.  0      –   255.255.255.240
      ------------------------  ------------------------
        0.   0.   0.255          0.   0.   0.  15
```

OSPF Single Area on IPv4 Network - Configuration

Router(config) # ip routing
Router(config) # router ospf < Process ID >
Router(config-router) # router-id < Router ID >
Router(config-router) # network < Network ID > <Wildcard mask> area <area ID >

OSPF Single Area on IPv4 Network

ZOOM TECHNOLOGIES



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16
S 0/1	172.18.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	172.17.0.0/16
S 0/0/1	172.16.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	172.18.0.0/16
S 0/1	172.17.0.0/16

CCIE CCNP CCNA

OSPF Single Area on IPv4 Network - Configuration

ZOOM TECHNOLOGIES

CHE

```
CHE (config) # ip routing
CHE (config) # router ospf 1
CHE (config-router) # router-id 1.1.1.1
CHE (config-router) # network 192.168.201.0 0.0.0.255 area 0
CHE (config-router) # network 172.16.0.0 0.0.255.255 area 0
CHE (config-router) # network 172.18.0.0 0.0.255.255 area 0
CHE (config-router) # end
CHE #
```

BAN

```
BAN (config) # ip routing
BAN (config) # router ospf 3
BAN (config-router) # router-id 3.3.3.3
BAN (config-router) # network 192.168.203.0 0.0.0.255 area 0
BAN (config-router) # network 172.17.0.0 0.0.255.255 area 0
BAN (config-router) # network 172.18.0.0 0.0.255.255 area 0
BAN (config-router) # end
BAN #
```

HYD-1

```
HYD-1 (config) # ip routing
HYD-1 (config) # router ospf 2
HYD-1 (config-router) # router-id 2.2.2.2
HYD-1 (config-router) # network 192.168.202.0  0.255.255.255 area 0
HYD-1 (config-router) # network 172.16.0.0  0.0.255.255 area 0
HYD-1 (config-router) # network 172.17.0.0 0.0.255.255 area 0
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

CCIE CCNP CCNA

OSPF Single Area on IPv4 Network - Verification

Verify the routing table

Router # show ip route

To verify the protocols

Router # show ip protocols

To check Neighbor Table

Router # show ip ospf neighbor

To check Database Table

Router # show ip ospf database

Link State Advertisement (LSA)

- Link
  - Router interface
- State
  - Description of interface and neighbor relation and sending to neighbor routers.
- LSAs are additionally refreshed every 30 minutes.

OSPF Packet types

- HELLO
  - To Discover the neighbor
  - To form neighbor relation
  - Keep Alive mechanism
- DBD
  - Database description the update are exchanged .
- LSR - Link state Request
  - Used for requesting for a newer updated information.
- LSU – Link State Update
  - Receiving the updated information from neighbors and link state update
- LSACK - Link State Acknowledgement
  - Once receiving the update sends thanks for information called as link state acknowledgement

OSPF Hello Packets

To verify the OSPF Hello & Dead Timers

Router # show ip protocols

Verify OSPF Hello Packets

Router # terminal monitor

Router # debug ip ospf hello

Passive interface

- **Passive interface is configured to stop the hello packets from exiting out of the interface.**
- **If passive interface is configured between the routers no neighbor relationship will be formed and no updates will be exchanged.**

Configure Passive interface

Router(config) # router ospf <pid>

Router(config-router) # passive-interface <interface type> <no.>


```
HYD-1 (config) # router ospf 2
HYD-1 (config-router) #  passive-interface FastEthernet0/0
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

OSPF Metric

- OSPF uses the cost as metric.
- Cost = Reference Bandwidth / interface Bandwidth.
- The default reference bandwidth is 100 Mbps
  - 100 Mbps cost = 100Mbps/100Mbps = 1
  - 1.544Mbps cost = 100Mbps/1.544Mbps = 64

Interface	Bandwidth (Kbps)	OSPF Cost
Serial	1544	64
Ethernet	10000	10
FastEthernet	100000	1
GigabitEthernet	1000000	1

OSPF Cost metric for an interface

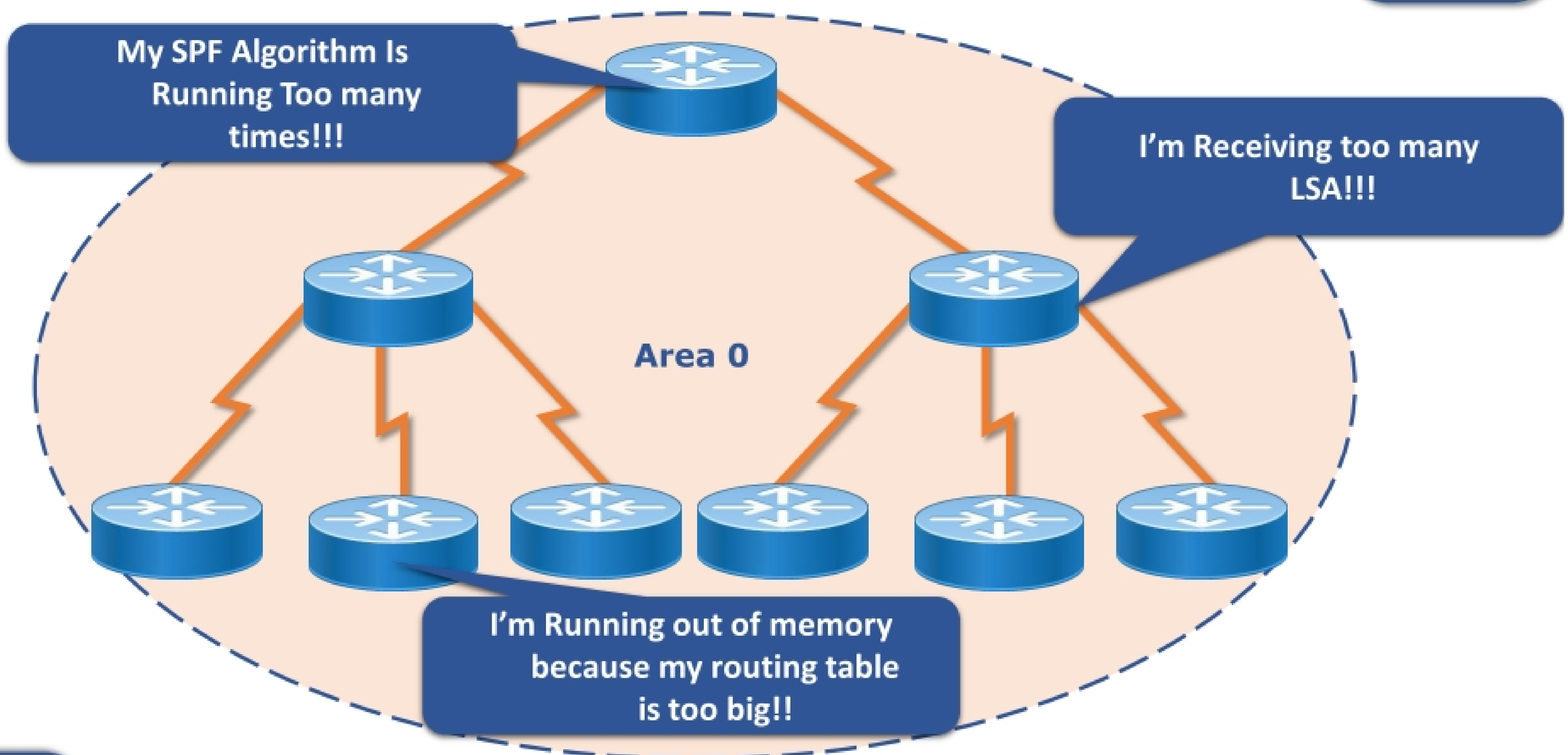
Router(config) # interface <interface type> <no.>

Router(config-if) # ip ospf cost <cost>


```
HYD-1 (config) # interface serial 0/0/0
HYD-1 (config-router) # ip ospf cost 100
HYD-1 (config-router) # end
```

Network Diagram

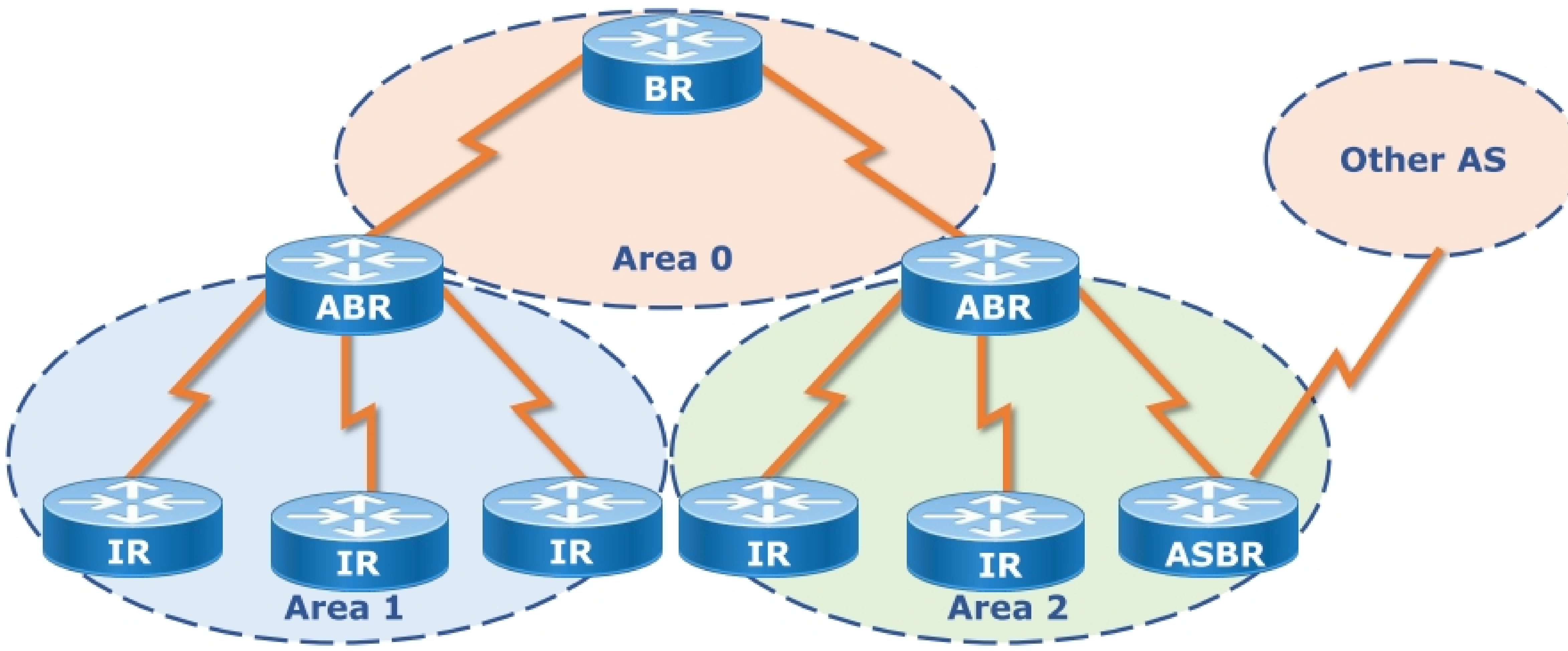
Issues with OSPF single area



Hierarchical Network Design using Areas

- **OSPF Network Design is divided into multiple areas**
- **One area has to be designated as Area 0**
- **Area 0 is called the Backbone Area**
- **Remaining Areas are called as non back bone area.**

OSPF Multiple Area



Types of Routers

- Backbone Router (BR)
  - The router which belongs to backbone area is called as Backbone router
- Internal Router (IR)
  - The router which belongs to regular area is called Internal Router
- Area Border Router (ABR)
  - The router which shares two different areas is called Area Border Router
- Autonomous System Border Router (ASBR)
  - The router which is connected to different protocol is called Autonomous system boundary router.

OSPF Multiple Area on IPv4 Network - Configuration

ZOOM TECHNOLOGIES

Router(config) # ip routing

Router(config) # router ospf < Process ID >

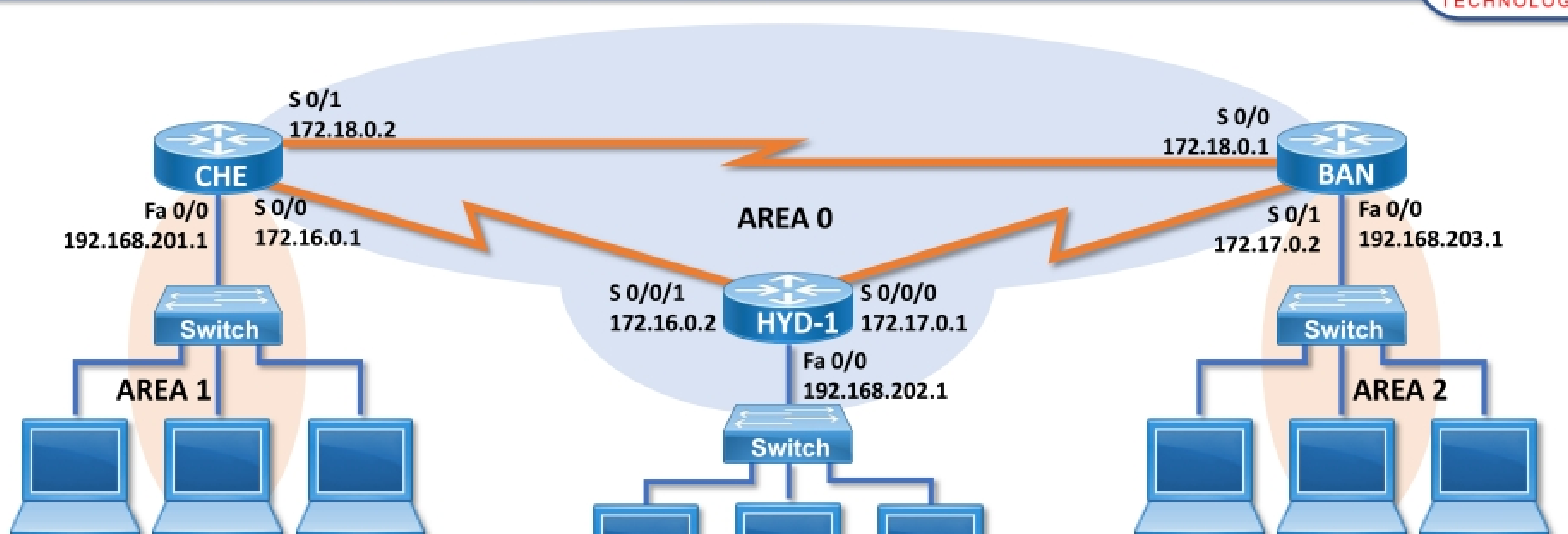
Router(config-router) # router-id < Router ID >

Router(config-router) # network < Network ID > <Wildcard mask> area <Area ID >

CCIE CCNP CCNA

OSPF Multiple Area on IPv4 Network

ZOOM TECHNOLOGIES



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16
S 0/1	172.18.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	172.17.0.0/16
S 0/0/1	172.16.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	172.18.0.0/16
S 0/1	172.17.0.0/16

CCIE CCNP CCNA

OSPF Multiple Area on IPv4 Network - Configuration

ZOOM TECHNOLOGIES

CHE

```
CHE (config) # ip routing
CHE (config) # router ospf 1
CHE (config-router) # router-id 1.1.1.1
CHE (config-router) # network 192.168.201.0 0.0.0.255 area 1
CHE (config-router) # network 172.16.0.0 0.0.255.255 area 0
CHE (config-router) # network 172.18.0.0 0.0.255.255 area 0
CHE (config-router) # end
CHE #
```

BAN

```
BAN (config) # ip routing
BAN (config) # router ospf 3
BAN (config-router) # router-id 3.3.3.3
BAN (config-router) # network 192.168.203.0 0.0.0.255 area 2
BAN (config-router) # network 172.17.0.0 0.0.255.255 area 0
BAN (config-router) # network 172.18.0.0 0.0.255.255 area 0
BAN (config-router) # end
BAN #
```

HYD-1

```
HYD-1 (config) # ip routing
HYD-1 (config) # router ospf 2
HYD-1 (config-router) # router-id 2.2.2.2
HYD-1 (config-router) # network 192.168.202.0  0.255.255.255 area 0
HYD-1 (config-router) # network 172.16.0.0  0.0.255.255 area 0
HYD-1 (config-router) # network 172.17.0.0 0.0.255.255 area 0
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

CCIE CCNP CCNA

OSPF Multiple Area on IPv4 Network - Verification

ZOOM TECHNOLOGIES

Verify the routing table

Router # show ip route

To verify the protocols

Router # show ip protocols

To check Neighbor Table

Router # show ip ospf neighbor

To check Database Table

Router # show ip ospf database

CCIE CCNP CCNA

OSPFv3 Characteristics

- RFC 2740
- Multicast address is FF02::5 and FF02::6
- Ospfv3 is configured on link basis.
- OSPFv3 supports multiple instances on a single link.
- OSPFv3 adjacencies are formed using link-local address.
- Still uses the router-id from IPv4

OSPFv3 on IPv6 Network - Configuration

Router(config) # ipv6 unicast-routing

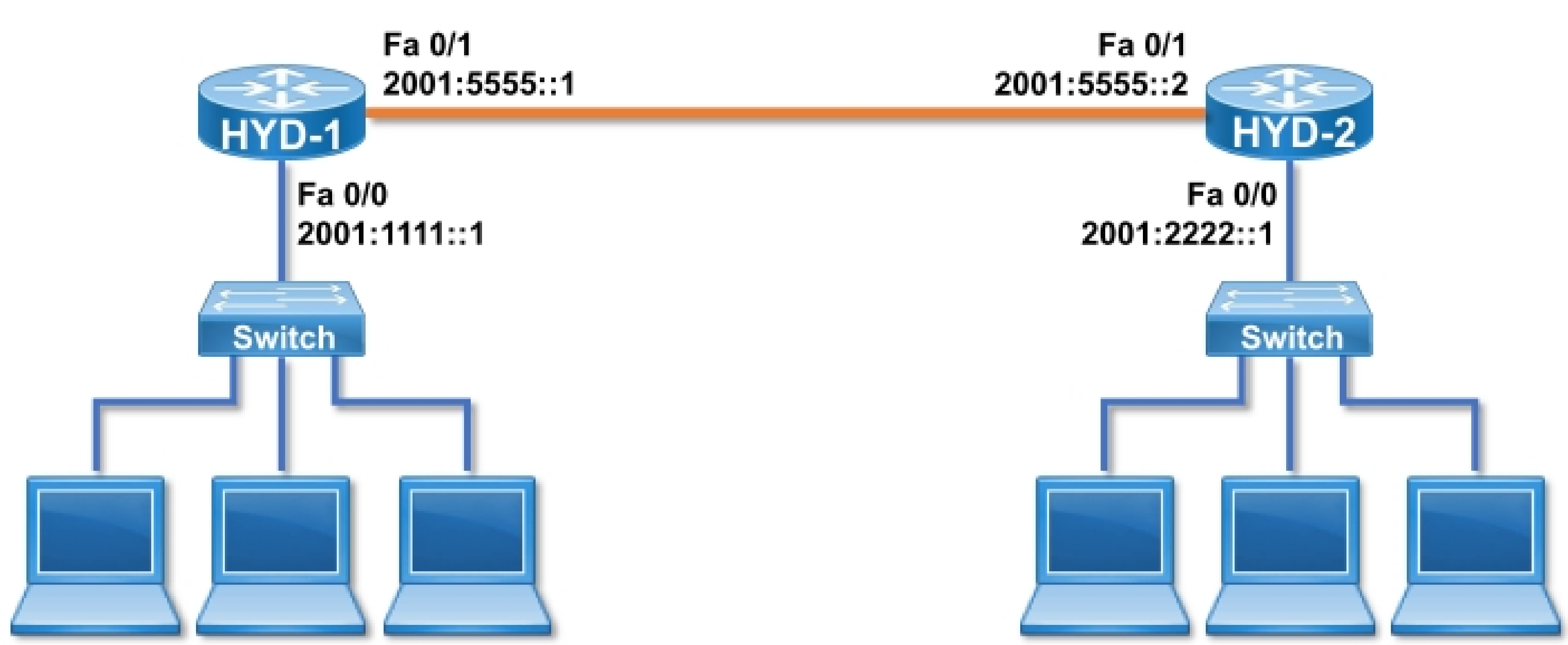
Router(config) # ipv6 router ospf <Process id>

Router(config-router) # router-id < Router ID >

Router(config) # interface < interface type > < no. >

Router(config-if) # ipv6 ospf <Process id> area <Area ID >

OSPFv3 on IPv6 Network



Interface	Network ID / Mask
Fa 0/0	2001:1111::/64
Fa 0/1	2001:5555::/64

Interface	Network ID / Mask
Fa 0/0	2001:2222::/64
Fa 0/1	2001:5555::/64

OSPFv3 on IPv6 Network - Configuration

HYD-1

```
HYD-1 (config) # ipv6 unicast-routing
HYD-1 (config) # ipv6 router ospf 2
HYD-1 (config-rtr) # router-id 11.11.11.11
HYD-1 (config-rtr) # exit
HYD-1 (config) # interface fastethernet 0/0
HYD-1 (config-if) # ipv6 ospf 2 area 0
HYD-1 (config-if) # exit
HYD-1 (config) # interface fastethernet 0/1
HYD-1 (config-if) # ipv6 ospf 2 area 0
HYD-1 (config-if) # end
HYD-1 #
```

HYD-2

```
HYD-2 (config) # ipv6 unicast-routing
HYD-2 (config) # ipv6 router ospf 2
HYD-2 (config-rtr) # router-id 22.22.22.22
HYD-2 (config-rtr) # exit
HYD-2 (config) # interface fastethernet 0/0
HYD-2 (config-if) # ipv6 ospf 2 area 0
HYD-2 (config-if) # exit
HYD-2 (config) # interface fastethernet 0/1
HYD-2 (config-if) # ipv6 ospf 2 area 0
HYD-2 (config-if) # end
HYD-2 #
```

Network Diagram

OSPFv3 on IPv6 Network - Verification

Verify the routing table

Router # show ipv6 route

Network Diagram

Disadvantages of OSPF

- Consumes more Memory and CPU processing time
- Complex configuration

EIGRP Characteristics

- Advanced Distance Vector Routing Protocol
- Open Standard, was cisco proprietary
- Diffusing update algorithm (DUAL)
- Classless Routing Protocol
- Metric = Composite Metric
  - Bandwidth, Load, Delay, Reliability, MTU
- Updates are sent as multicast(224.0.0.10) or unicast
- EIGRP protocol alone supports equal and unequal cost load balancing.
- Default of 4 paths and maximum of 16 paths

EIGRP Characteristics

- Administrative Distance is 90
- Maximum Hop Count is 255 (Default 100)
- Hello timer – 5 seconds, Hold on timer - 15seconds
- Supports multiple Routed Protocols - IP, IPX, Apple talk
- EIGRP protocol number 88.

EIGRP Tables

- Neighbor Table
  - Contains information about directly connected neighbors.

- Topology Table
  - Contains entries for all destinations, along with the feasible distance and the advertised distance.
  - Contains the successors.
  - Contains feasible successor if any.

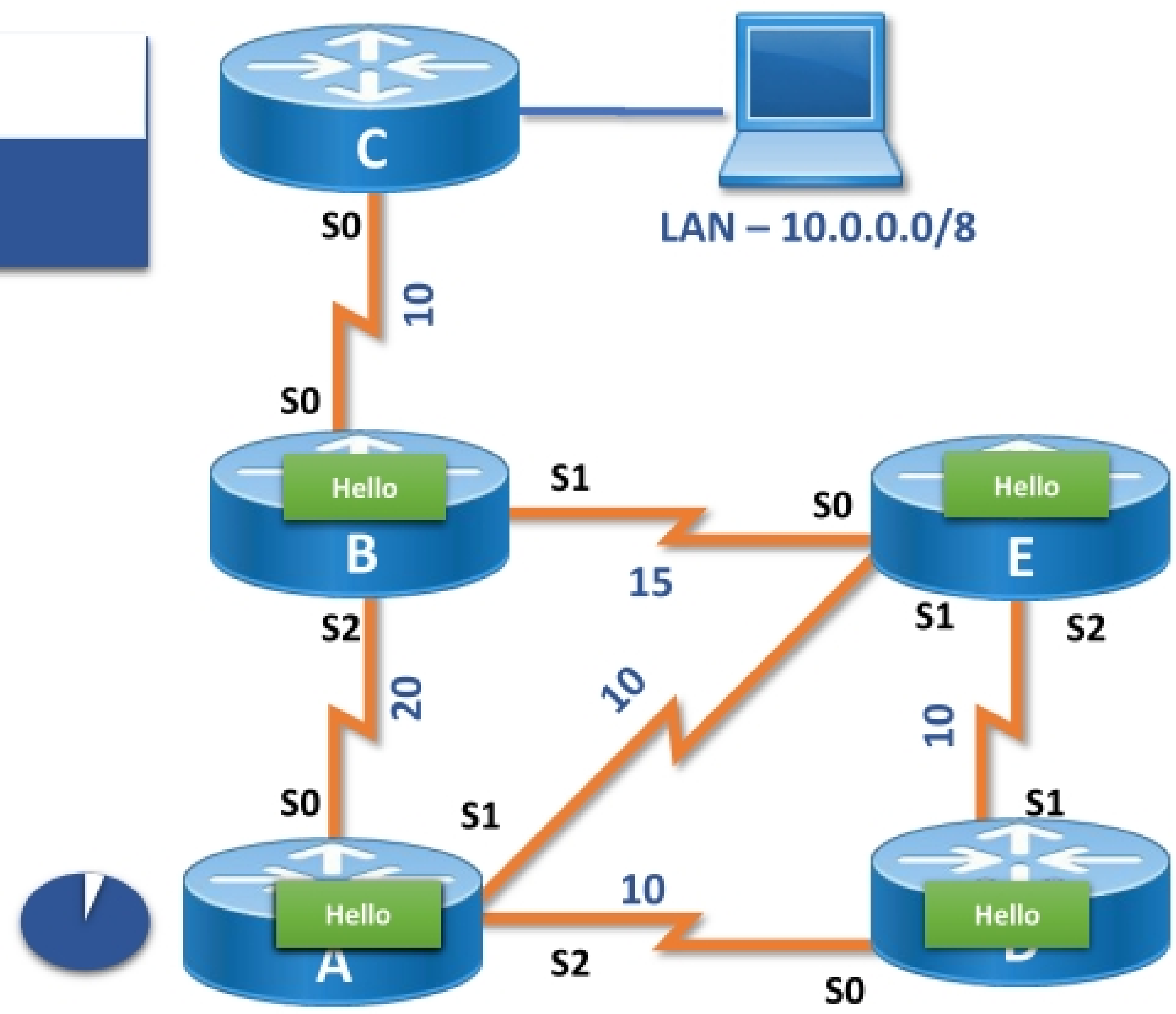
- Routing Table
  - Entries with the best path for each destination from the Topology table are moved into the Routing Table

EIGRP Terminology

- Feasible Distance FD :
  - Feasible distance (FD) is the metric of the best route to a destination, including the local link distance.
  - Feasible distance = advertised distance + local link distance (of the best path)
- Advertised Distance AD:
  - The distance of a route as advertised by the neighbor. It does not include the local link distance.
- Successor :
  - The neighbor with best distance to the destination.
- Feasible Successor :
  - The neighbor with second best distance to the destination, which meets this criteria: advertised distance should be less than the feasible distance (AD <FD)

EIGRP - Neighbor Table

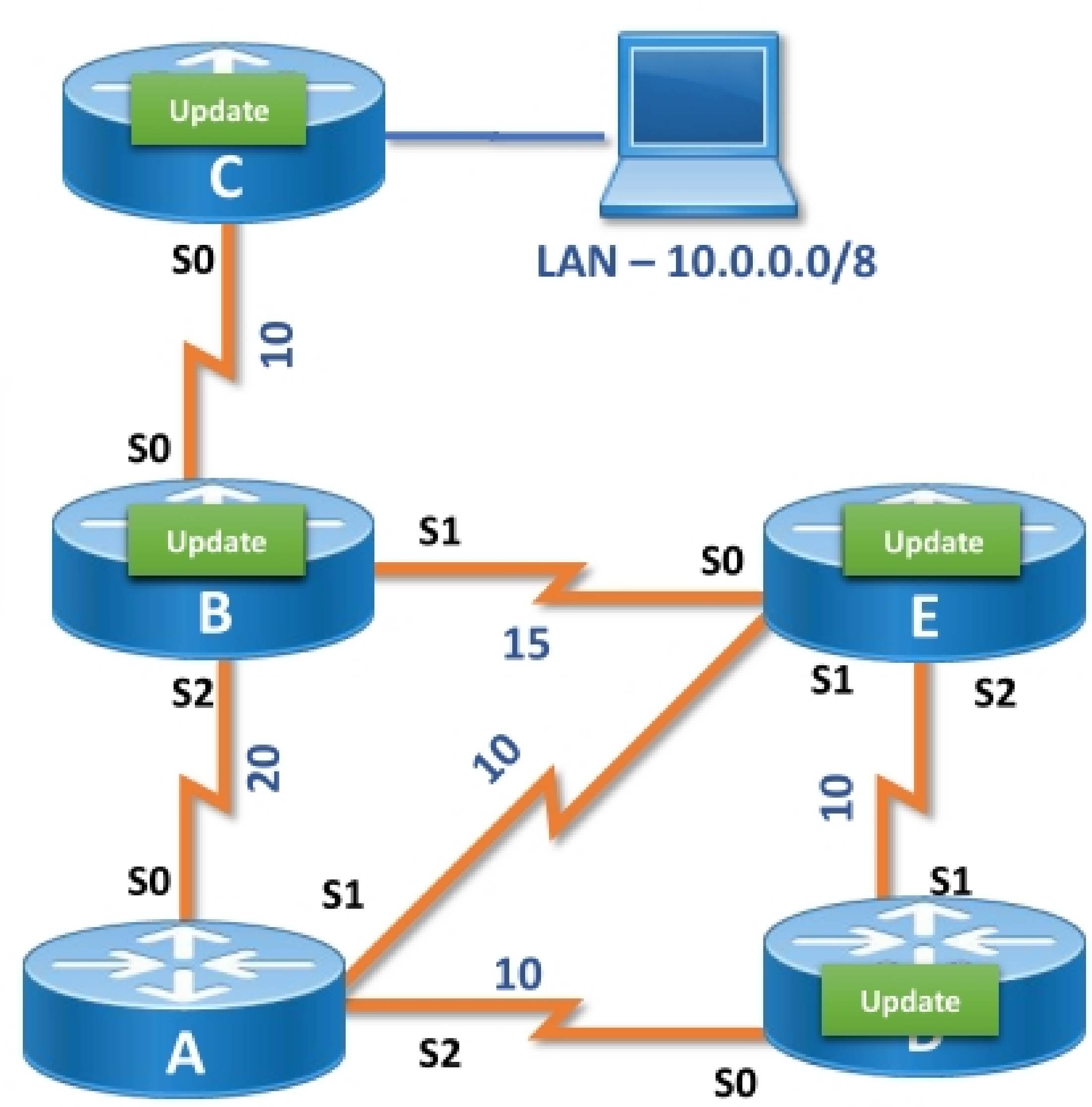
NEIGHBOR TABLE (Router A)	
Neighbor	Interface
B	S0
D	S2
E	S1



EIGRP - Topology Table

NEIGHBOR TABLE (Router A)	
Neighbor	Interface
B	S0
D	S2
E	S1

TOPOLOGY TABLE (Router A)					
Network	Neighbor	TD	AD	FD	
10.0.0.0/8	via B	30	10	30	S
	via E	35	25		FS
	via D	45	35		

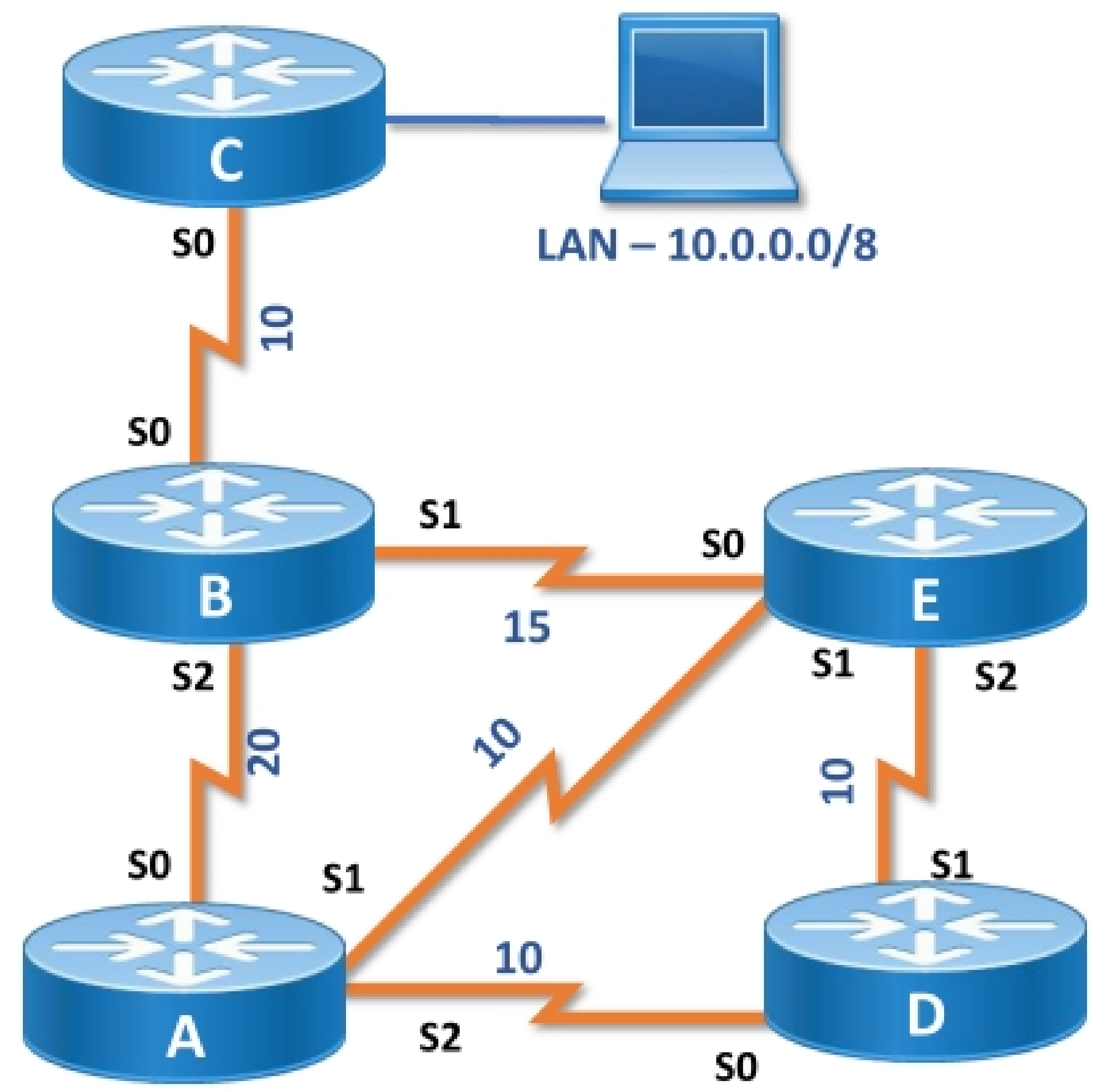


EIGRP - Routing Table

NEIGHBOR TABLE (Router A)	
Neighbor	Interface
B	S0
D	S2
E	S1

TOPOLOGY TABLE (Router A)					
Network	Neighbor	TD	AD	FD	
10.0.0.0/8	via B	30	10	30	S
	via E	35	25		FS
	via D	45	35		

ROUTING TABLE (Router A)
D 10.0.0.0/8 [90/30] via B, 01:36, Serial0



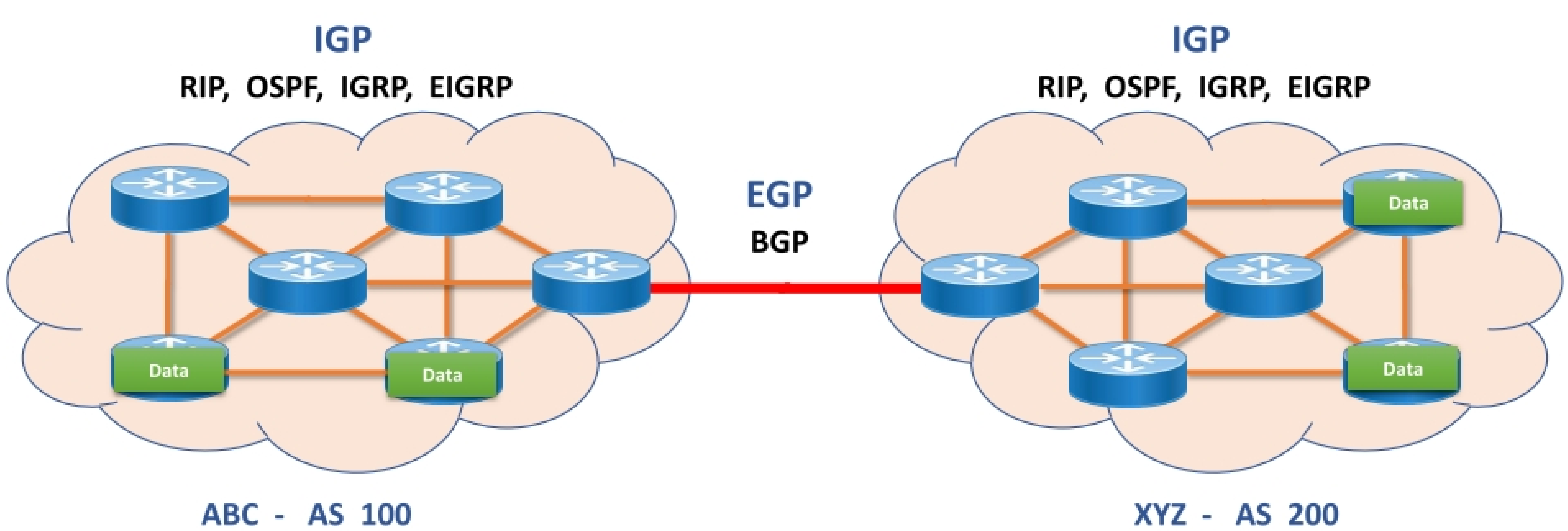
Autonomous System

- Autonomous system is a collection of routers under one common administration
- Autonomous system is identified by numbers
- Autonomous system ranges from 0-65535
  - Public - 1-64511
  - Private - 64512-65535

Routing Protocol Classification

IGP	EGP
• Interior Gateway Protocol • Routing protocols used within an Autonomous system • Ex: RIP, IGRP, EIGRP, OSPF, IS-IS	• Exterior Gateway Protocol • Routing protocol used between different Autonomous systems • Ex: Border Gateway Protocol is extensively used as EGP

IGP and EGP



- IGPs operate within an autonomous system
- EGPs connect different autonomous systems

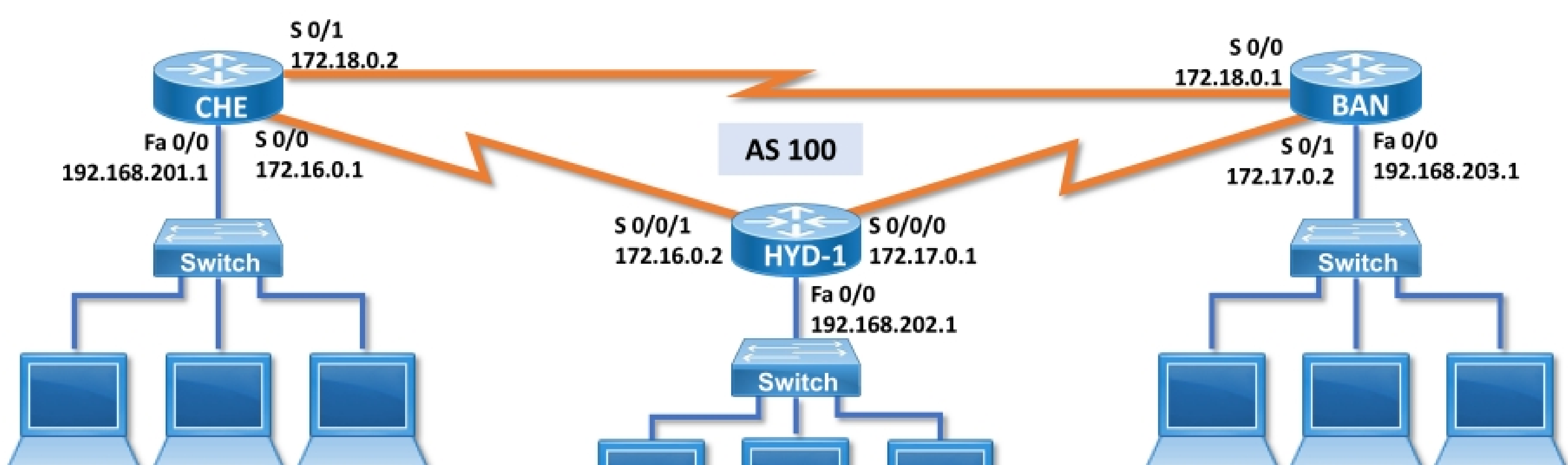
EIGRP on IPv4 Network - Configuration

Router(config) # ip routing

Router(config) # router eigrp < AS No >

Router(config-router) # network < Network ID > <Wildcard mask>

EIGRP on IPv4 Network



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16
S 0/1	172.18.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	172.17.0.0/16
S 0/0/1	172.16.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	172.18.0.0/16
S 0/1	172.17.0.0/16

EIGRP on IPv4 Network - Configuration

CHE

```
CHE (config) # ip routing
CHE (config) # router eigrp 100
CHE (config-router) # network 192.168.201.0  0.0.0.255
CHE (config-router) # network 172.16.0.0  0.0.255.255
CHE (config-router) # network 172.18.0.0  0.0.255.255
CHE (config-router) # end
CHE #
```

BAN

```
BAN (config) # ip routing
BAN (config) # router eigrp 100
BAN (config-router) # network 192.168.203.0  0.0.0.255
BAN (config-router) # network 172.17.0.0  0.0.255.255
BAN (config-router) # network 172.18.0.0  0.0.255.255
BAN (config-router) # end
BAN #
```

HYD-1

```
HYD-1 (config) # ip routing
HYD-1 (config) # router eigrp 100
HYD-1 (config-router) # network 192.168.202.0  0.0.0.255
HYD-1 (config-router) # network 172.16.0.0  0.0.255.255
HYD-1 (config-router) # network 172.17.0.0  0.0.255.255
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

EIGRP on IPv4 Network - Verification

Verify the routing table

Router # show ip route

To verify the protocols

Router # show ip protocols

To check Neighbor Table

Router # show ip eigrp neighbor

To check Topology Table

Router # show ip eigrp topology

EIGRP Metric

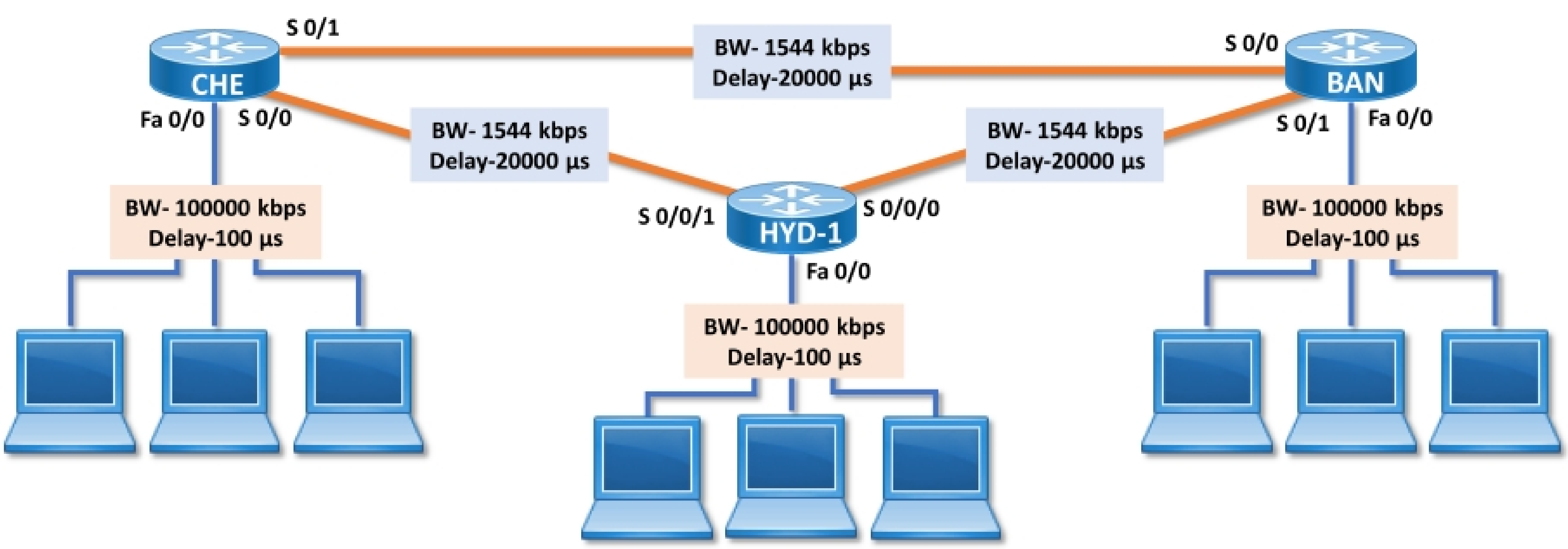
- EIGRP uses the default metric as Bandwidth and Delay

Metric = (BW + Delay) * 256

Metric = $((10^7$/ Lowest Bandwidth in kbps) + (Sum of Total Delay/10)} *256

Interface	Bandwidth (Kbps)	Delay (µs)
Serial	1544	20000
Ethernet	10000	1000
FastEthernet	100000	100
GigabitEthernet	1000000	10

EIGRP Metric Calculation



EIGRP Metric = $((10^7$/lowest Bandwidth in kbps) + (Sum of Total Delay/10)) *256

= (10000000/1544) + (20000 + 100 / 10) * 256

= 2172416

EIGRP Packets

To verify the EIGRP Hello & Holdown Timers

Router # show ip protocols

Verify EIGRP Packets

Router # terminal monitor

Router # debug eigrp packet

Passive interface

- Passive interface is configured to stop the hello packets from exiting out of the interface.
- If passive interface is configured between the routers no neighbor relationship will be formed and no updates will be exchanged.

Configure Passive interface

Router(config) # router eigrp <AS No>

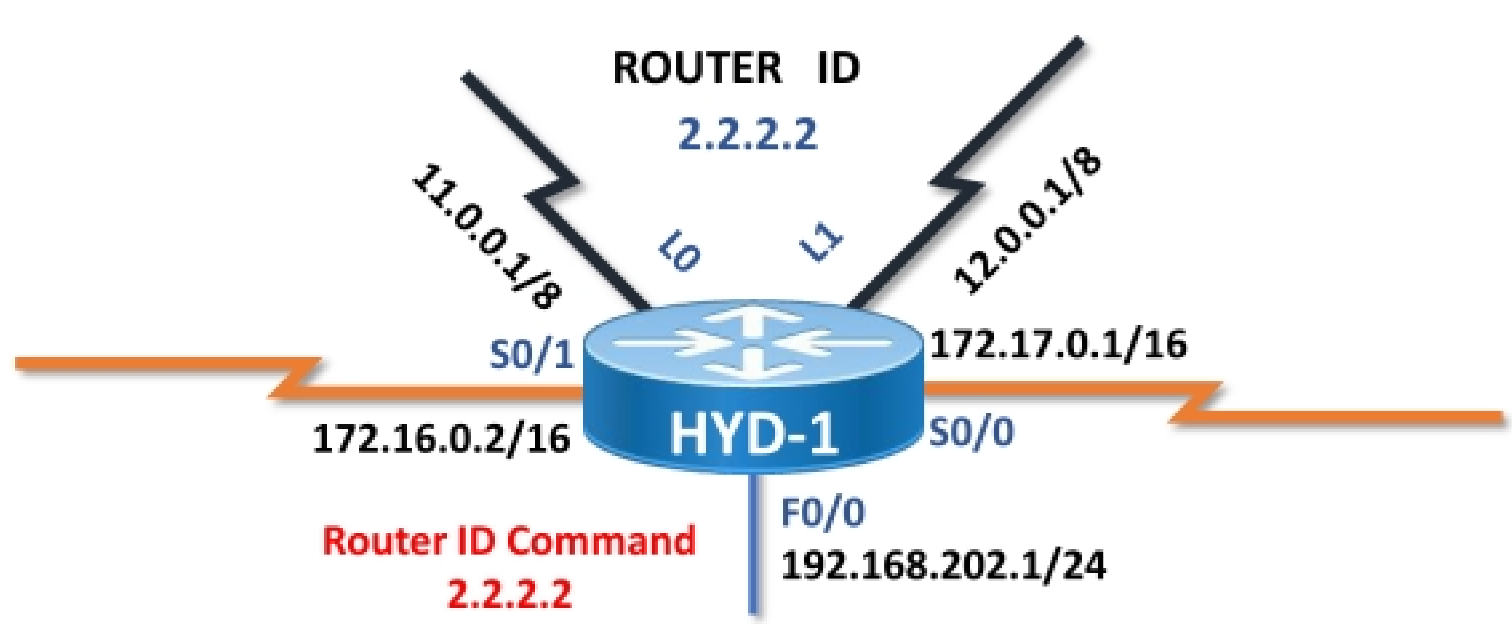
Router(config-router) # passive-interface <interface type> <no.>


```
HYD-1 (config) # router eigrp 100
HYD-1 (config-router) #  passive-interface FastEthernet0/0
HYD-1 (config-router) # end
HYD-1 #
```

Network Diagram

Router ID

- The router-id is used to identify the router in EIGRP
  - First preference is given to router-id command
  - Second preference is given to highest loopback interfaces configured on router
  - Third preference is given to highest physical ip address



Configure Router ID

```
Router(config) #  router eigrp  <AS No>
Router(config-router) #  eigrp router-id <router-id>
```


```
HYD-1 (config) # router eigrp 100
HYD-1 (config-router) # eigrp router-id 2.2.2.2
HYD-1 (config-router) # end
HYD-1  #
```

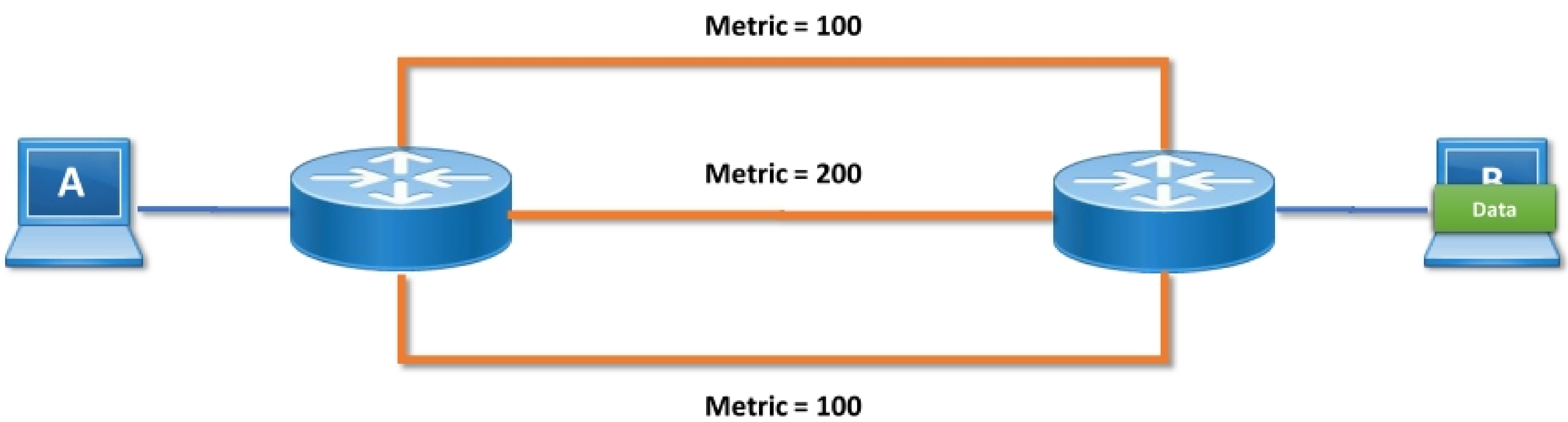
Network Diagram

EIGRP - Load Balancing

- EIGRP supports two types of load balancing
  - Equal cost load balancing
  - Unequal cost load balancing

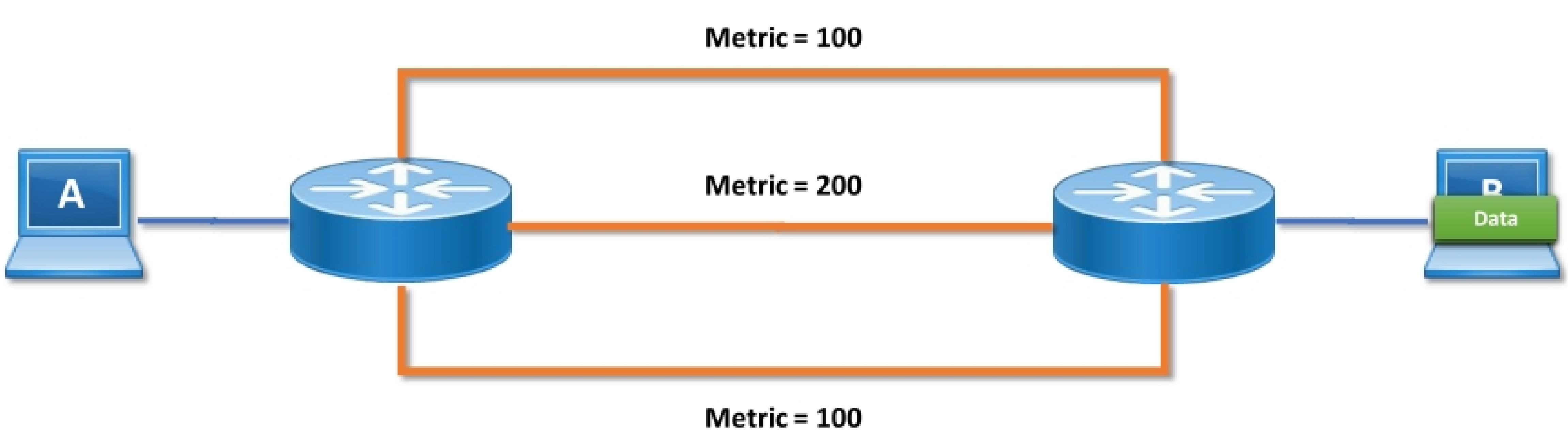
- Load balancing on 4 equal cost paths enabled(Default)
- Maximum paths are based on device platform (equal or unequal cost paths)

EIGRP - Equal Cost Load Balancing



EIGRP – Unequal Cost Load Balancing

- **By default it is turned off**



EIGRPv6 Characteristics

- RFC 7868
- Multicast Address for EIGRPv6 is FF02::A
- Still uses the router-id from IPv4

EIGRPv6 on IPv6 Network - Configuration

Router(config) # ipv6 unicast-routing

Router(config) # ipv6 router eigrp <AS No>

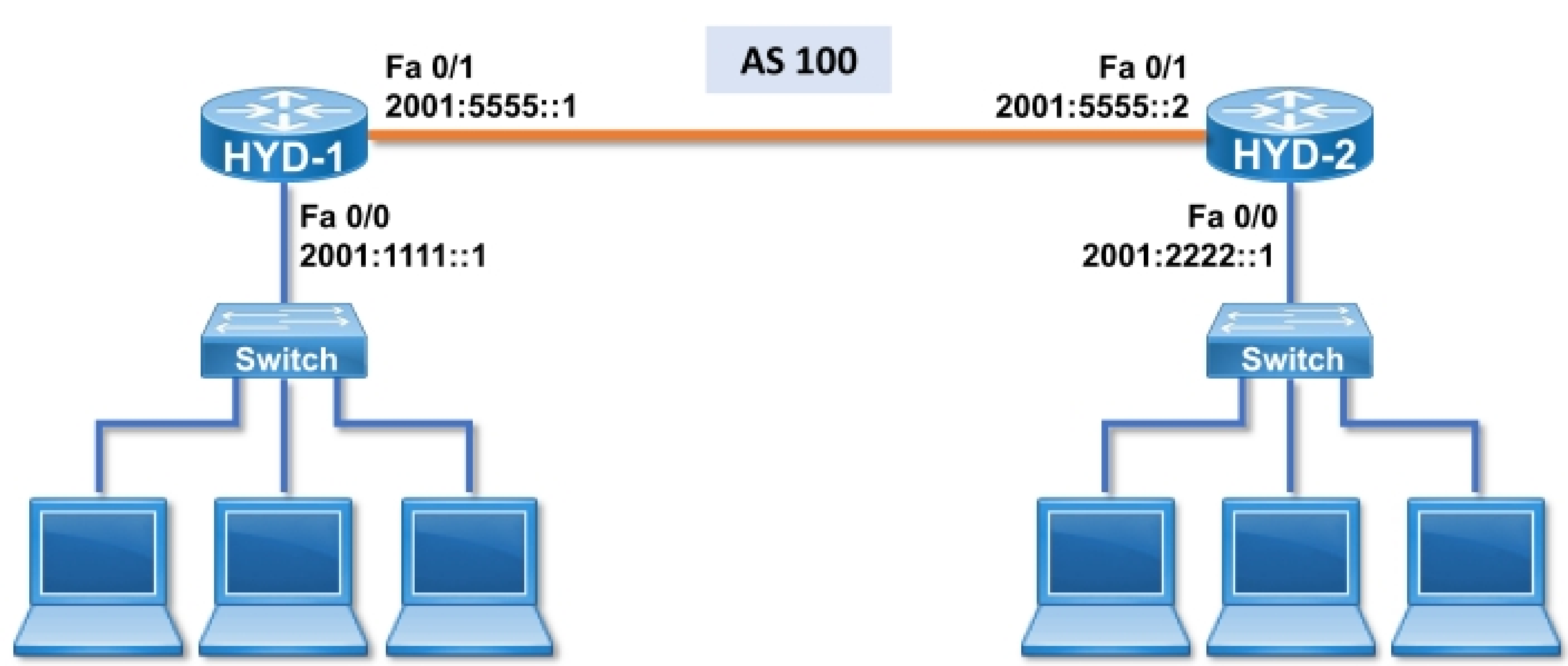
Router(config-router) # eigrp router-id <router-id>

Router(config-router) # exit

Router(config) # interface < interface type > < no. >

Router(config-if) # ipv6 eigrp <AS No>

EIGRPv6 on IPv6 Network



Interface	Network ID / Mask
Fa 0/0	2001:1111::/64
Fa 0/1	2001:5555::/64

Interface	Network ID / Mask
Fa 0/0	2001:2222::/64
Fa 0/1	2001:5555::/64

EIGRPv6 on IPv6 Network - Configuration

ZOOM TECHNOLOGIES

HYD-1

```
HYD-1 (config) # ipv6 unicast-routing
HYD-1 (config) # ipv6 router eigrp 100
HYD-1 (config-rtr) # eigrp router-id 11.11.11.11
HYD-1 (config-rtr) # exit
HYD-1 (config) # interface fastethernet 0/0
HYD-1 (config-if) # ipv6 eigrp 100
HYD-1 (config-if) # exit
HYD-1 (config) # interface fastethernet 0/1
HYD-1 (config-if) # ipv6 eigrp 100
HYD-1 (config-if) # end
HYD-1 #
```

HYD-2

```
HYD-2 (config) # ipv6 unicast-routing
HYD-2 (config) # ipv6 router eigrp 100
HYD-2 (config-rtr) # eigrp router-id 22.22.22.22
HYD-2 (config-rtr) # exit
HYD-2 (config) # interface fastethernet 0/0
HYD-2 (config-if) # ipv6 eigrp 100
HYD-2 (config-if) # exit
HYD-2 (config) # interface fastethernet 0/1
HYD-2 (config-if) # ipv6 eigrp 100
HYD-2 (config-if) # end
HYD-2 #
```

Network Diagram

CCIE CCNP CCNA

EIGRPv6 on IPv6 Network - Verification

ZOOM TECHNOLOGIES

Verify the routing table

Router # show ipv6 route

Network Diagram

CCIE CCNP CCNA

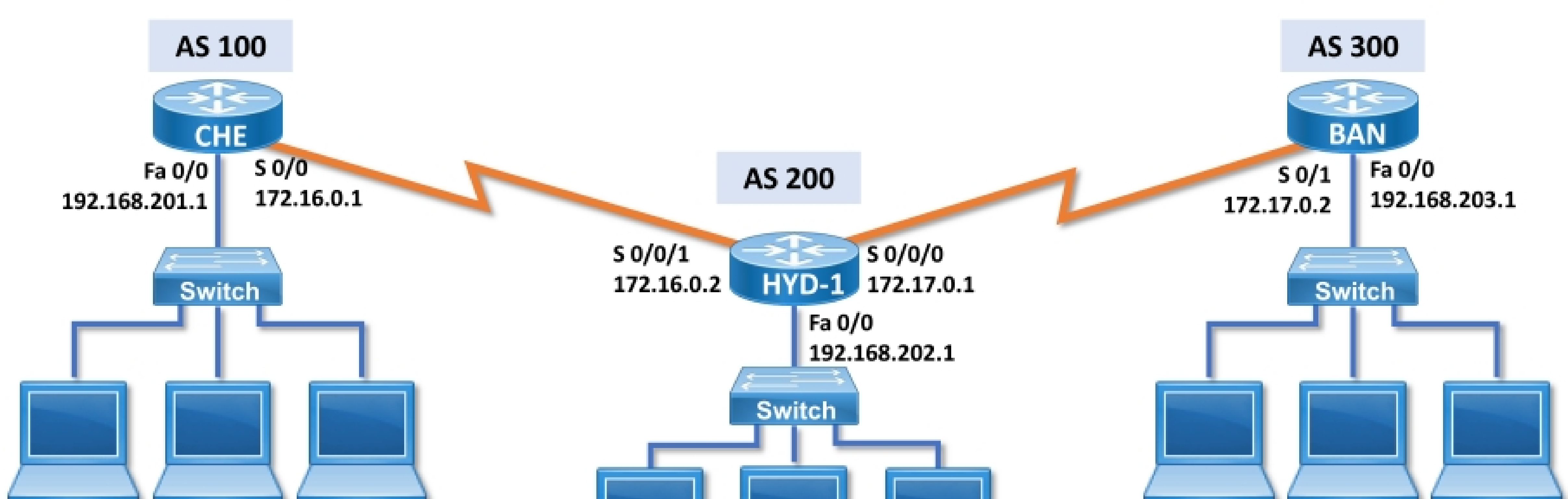
BGP Features

- Path Vector Protocol
- Open standard protocol
- Uses the path vector algorithm
- Classless routing protocol
- Administrative distance for EBGP is 20
- BGP exchanges routing information between Autonomous Systems
- External BGP (EBGP) which is also known as an inter-domain routing protocol, operates outside an AS and connects one AS to another.
- Hello timer is 60 seconds, Hold on timer is 180 seconds
- BGP uses the TCP port number 179.

EBGP on IPv4 Network - Configuration

Router(config) # ip routing
Router(config) # router bgp <AS No>
Router(config-router) # network < Network ID > mask <Subnet mask>
Router(config-router) # neighbor < peer address > remote-as < peer-as-no >
Router(config-router) # end

EBGP on IPv4 Network - Configuration



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	172.16.0.0/16
S 0/1	172.18.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	172.17.0.0/16
S 0/0/1	172.16.0.0/16

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	172.18.0.0/16
S 0/1	172.17.0.0/16

EBGP on IPv4 Network - Configuration

ZOOM TECHNOLOGIES

CHE

```
CHE (config) # ip routing
CHE (config) # router bgp 100
CHE (config-router) # network 192.168.201.0 mask 255.255.255.0
CHE (config-router) # network 172.16.0.0 mask 255.255.0.0
CHE (config-router) # neighbor 172.16.0.2 remote-as 200
CHE (config-router) # end
```

BAN

```
BAN (config) # ip routing
BAN (config) # router bgp 300
BAN (config-router) # network 192.168.203.0 mask 255.255.255.0
BAN (config-router) # network 172.17.0.0 mask 255.255.0.0
BAN (config-router) # neighbor 172.17.0.1 remote-as 200
BAN (config-router) # end
BAN (config) #
```

HYD-1

```
HYD-1 (config) # ip routing
HYD-1 (config) # router bgp 200
HYD-1 (config-router) # network 192.168.202.0 mask 255.255.255.0
HYD-1 (config-router) # network 172.16.0.0 mask 255.255.0.0
HYD-1 (config-router) # network 172.17.0.0 mask 255.255.0.0
HYD-1 (config-router) # neighbor 172.16.0.1 remote-as 100
HYD-1 (config-router) # neighbor 172.17.0.2 remote-as 300
HYD-1 (config-router) # end
```

CCIE CCNP CCNA

EBGP on IPv4 Network - Verification

ZOOM TECHNOLOGIES

Verify the routing table

Router # show ip route

To verify the BGP details

Router # show ip bgp summary

Router # show ip bgp

To check Neighbor Table

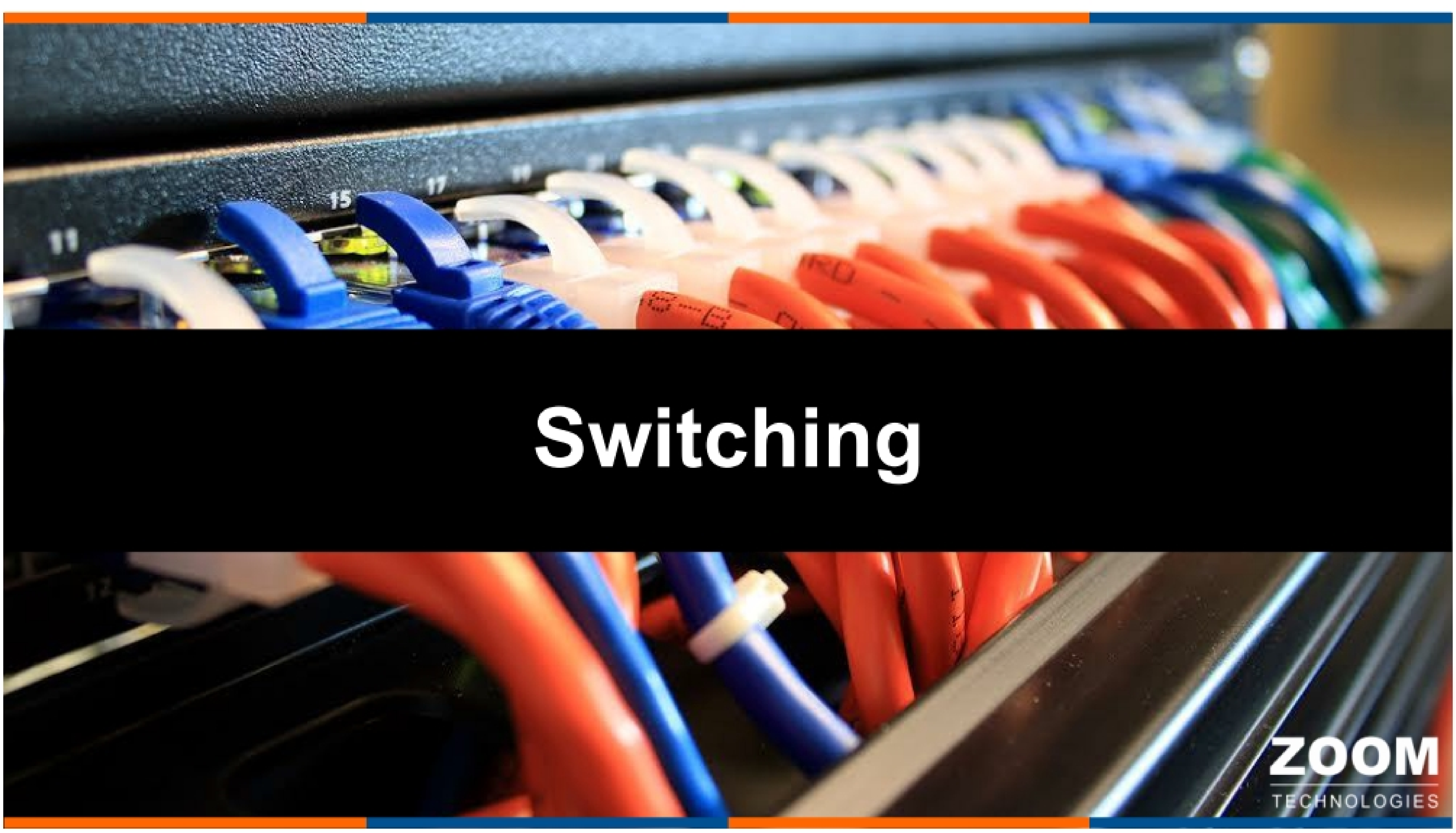
Router # show ip bgp neighbors

CCIE CCNP CCNA

Administrative Distance

- When ever multiple routing protocols are configured on a router to reach the same destination router makes use of Administrative Distance
- "Lesser the Administrative Distance more the Priority"

Routing Protocol	Administrative Distance
Directly connected	0
Static Route	1
EIGRP	90
OSPF	110
RIP	120
EBGP	20



Ethernet

- A technology originated by the University of Hawaii, later adopted by Xerox Corporation
- Ethernet is the most popular physical layer LAN technology.
- Ethernet standard known as IEEE Standard 802.3
- Ethernet speed is 10 Mbps.
- Types of Ethernet
  - Ethernet
  - FastEthernet
  - GigabitEthernet
  - 10 GigabitEthernet

FastEthernet

- The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds.
- FastEthernet speed is 100 Mbps.

Gigabit Ethernet

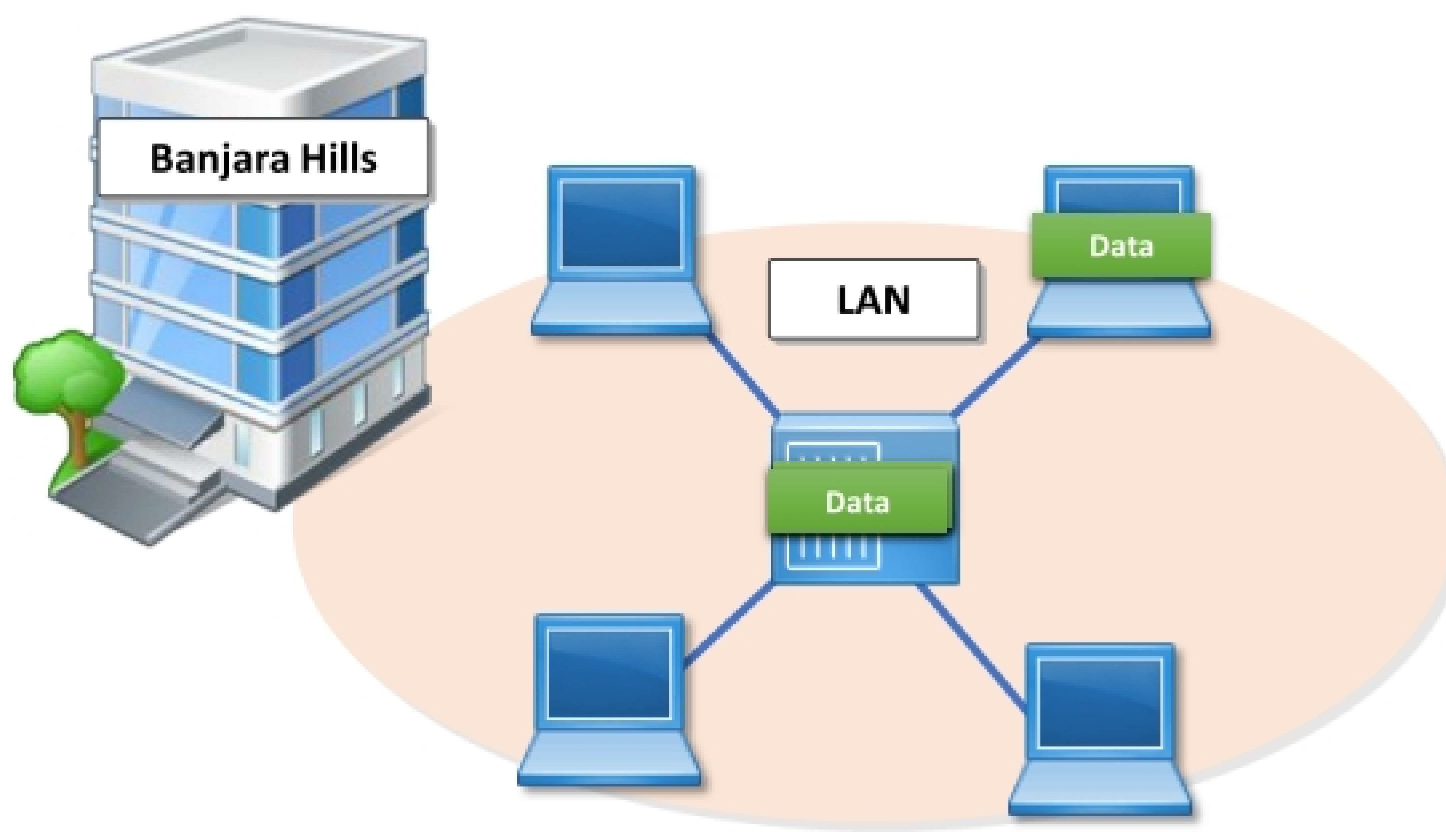
- Gigabit Ethernet was developed for faster communication networks with applications such as multimedia and Voice over IP (VoIP)
- Gigabit Ethernet standards are IEEE 802.3ab and IEEE 802.3z (optical fiber)
- Gigabit Ethernet speed is 1000 Mbps i.e. 1 Gbps

10 Gigabit Ethernet

- 10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards i.e. IEEE 802.3ae.
- 10 Gigabit Ethernet is based entirely on the use of optical fiber connections.
- 10 Gigabit Ethernet speed is 10000 Mbps i.e. 10 Gbps

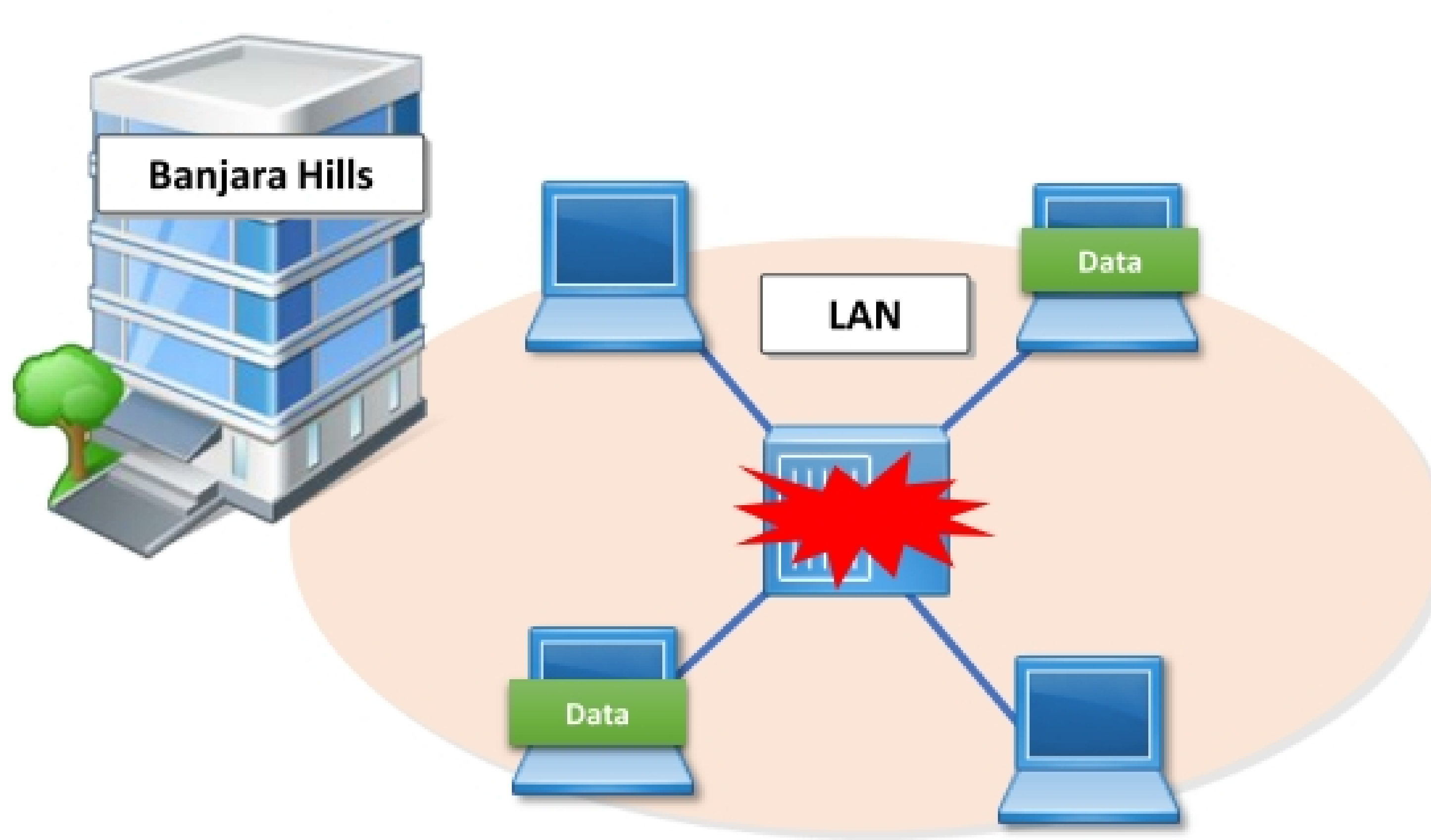
Broadcast Domain

- A broadcast domain is a set of network devices for which a broadcast frame sent by one device is received by all other devices in that LAN segment.



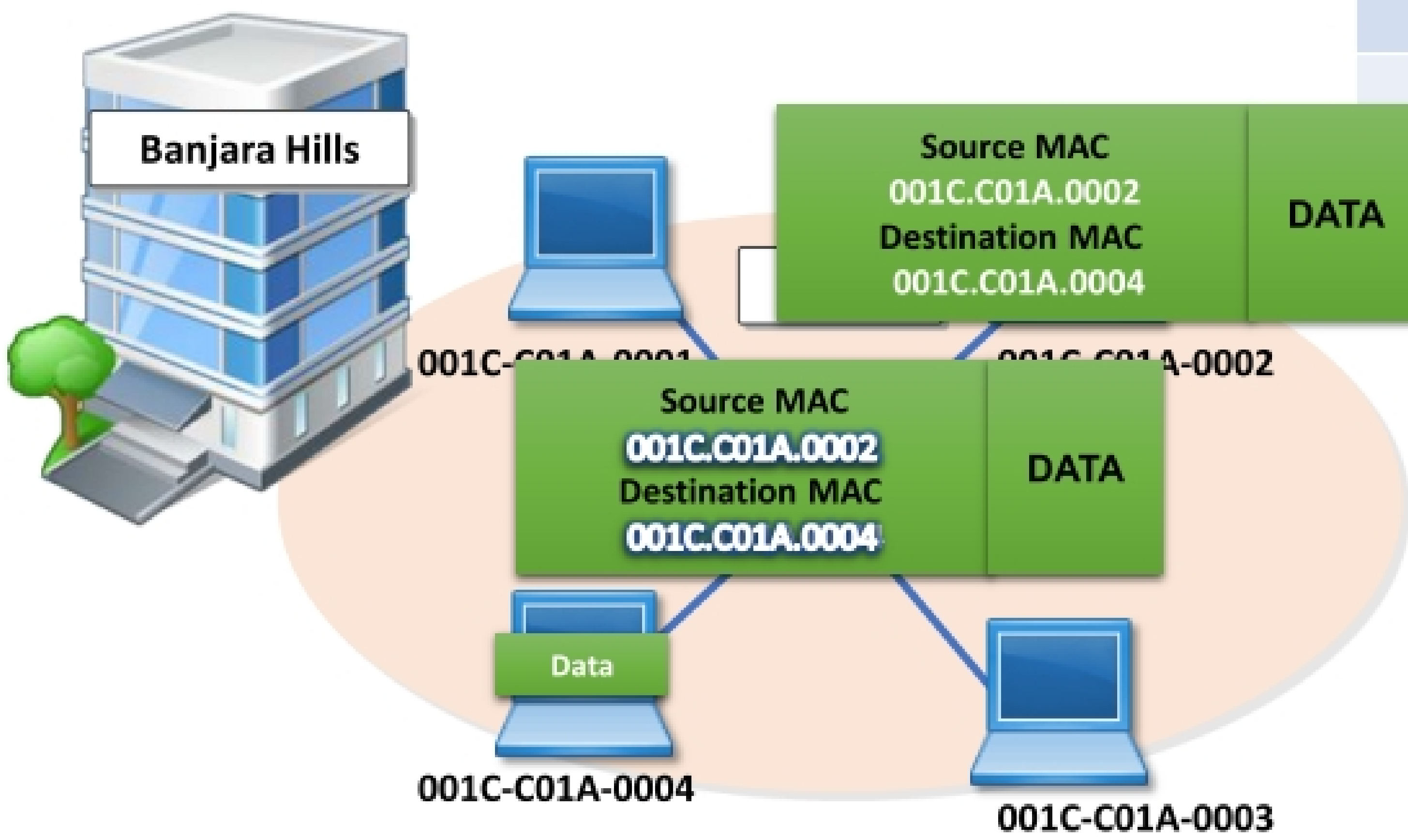
Collision Domain

- A collision domain is a set of network devices for which a frame sent by one device could result in a collision with a frame sent by any other device in the same LAN segment.



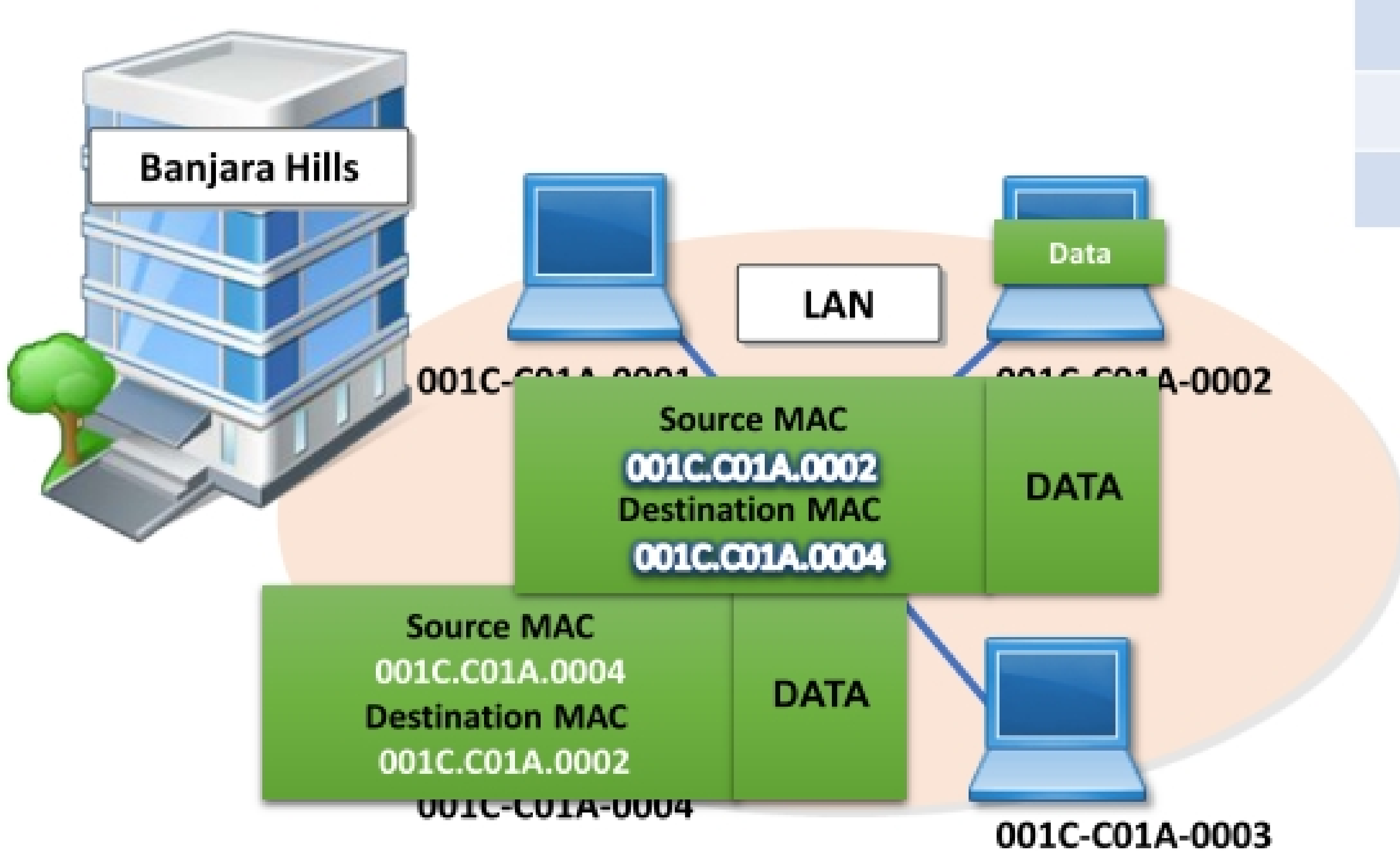
How Switch works ?

MAC ADDRESS TABLE	
PORT	MAC-ADDRESS
Fa0/1	
Fa0/2	001C-C01A-0002
Fa0/3	
Fa0/4	



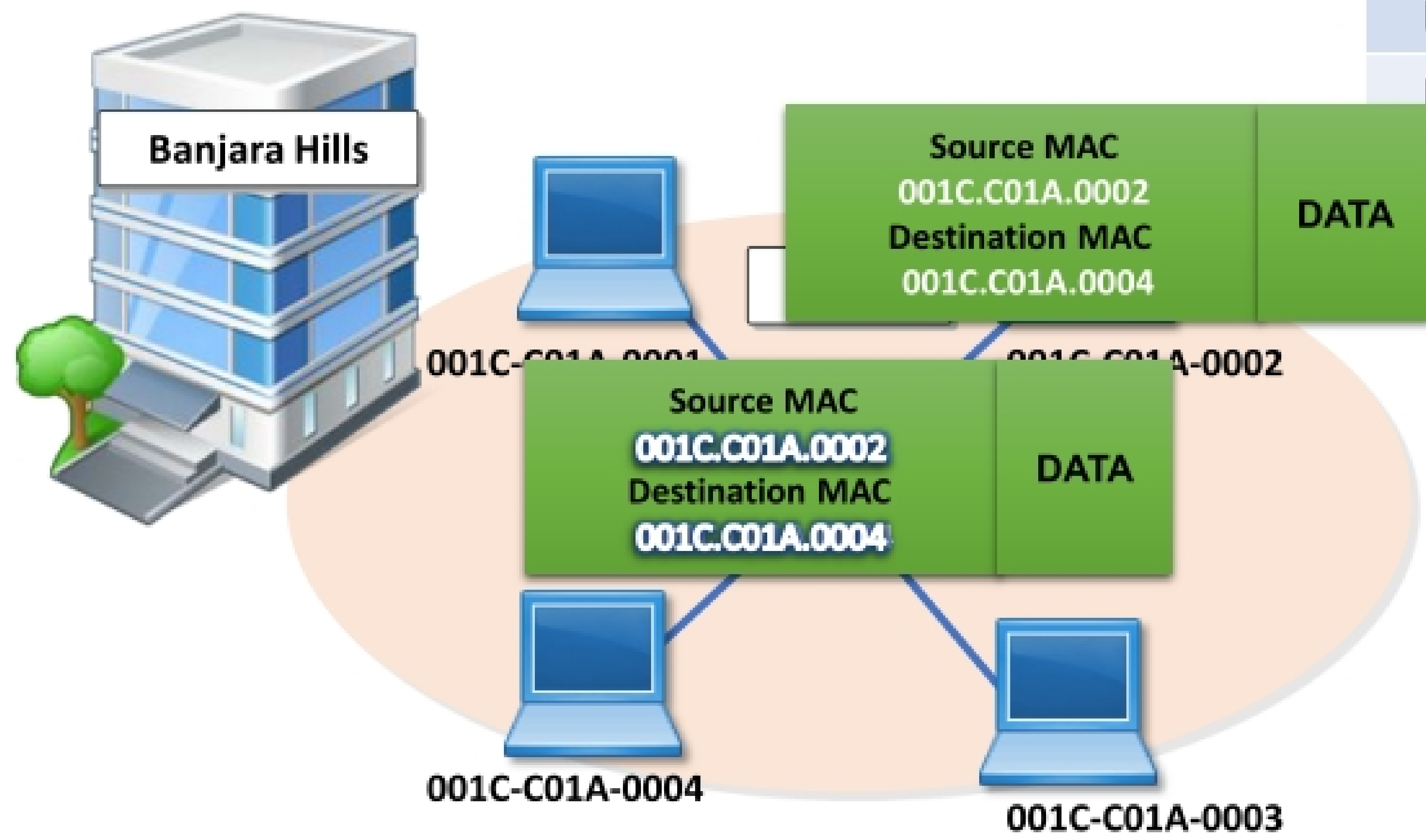
How Switch works ?

MAC ADDRESS TABLE	
PORT	MAC-ADDRESS
Fa0/1	
Fa0/2	001C-C01A-0002
Fa0/3	
Fa0/4	001C-C01A-0004



How Switch works ?

MAC ADDRESS TABLE	
PORT	MAC-ADDRESS
Fa0/1	
Fa0/2	001C-C01A-0002
Fa0/3	
Fa0/4	



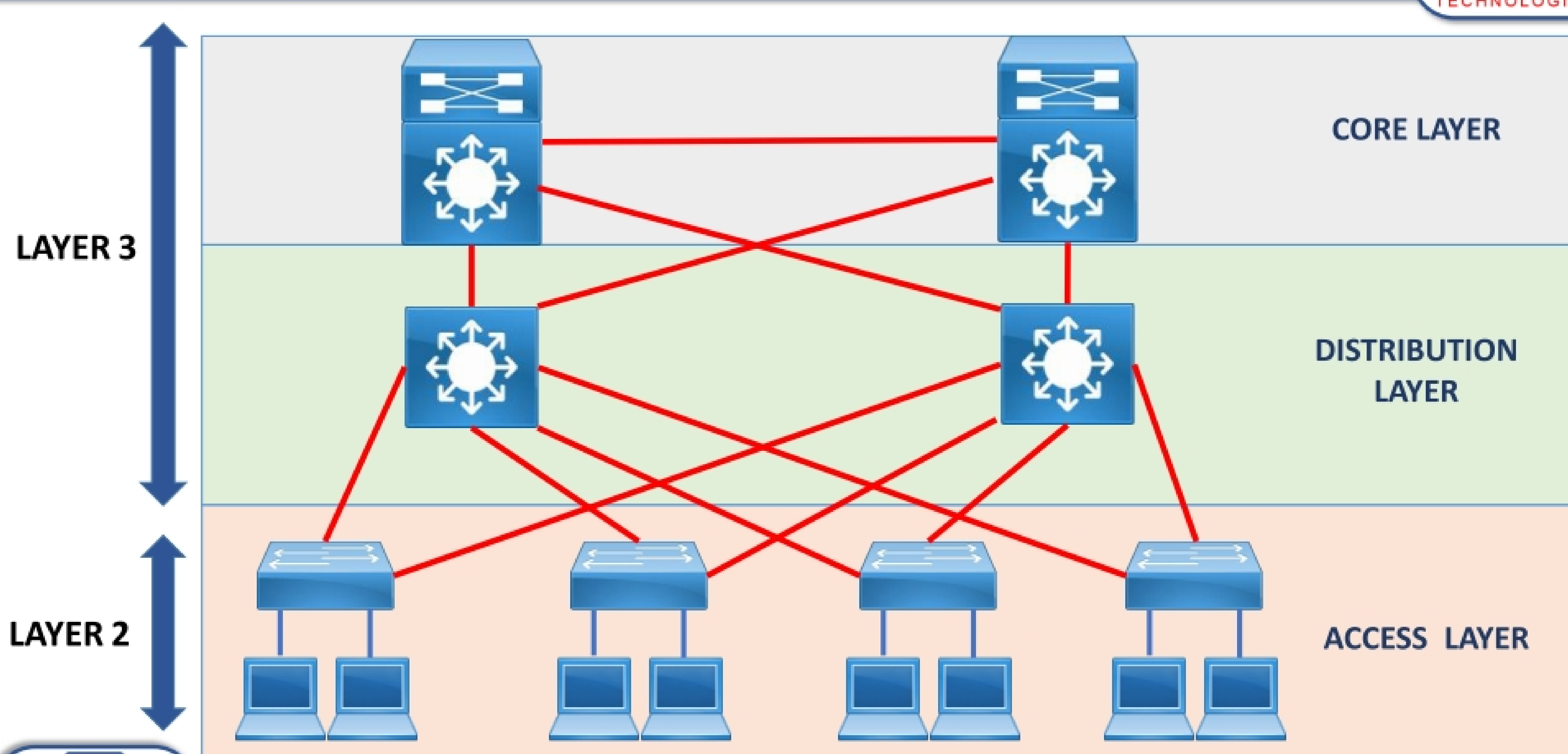
Types of Switches

- Manageable switches
  - On a Manageable switch an IP address can be assigned and configurations can be made. It has a console port .
- Unmanageable switches
  - On an Unmanageable switch configurations cannot be made, an IP address cannot be assigned as there is no console port.

Campus Network

- Campus is a LAN network supporting larger buildings or multiple buildings close to a specific area
- Cisco uses three terms to describe the role of each switch in a campus design.
  - Access Layer
  - Distribution Layer
  - Core Layer

Hierarchical Design

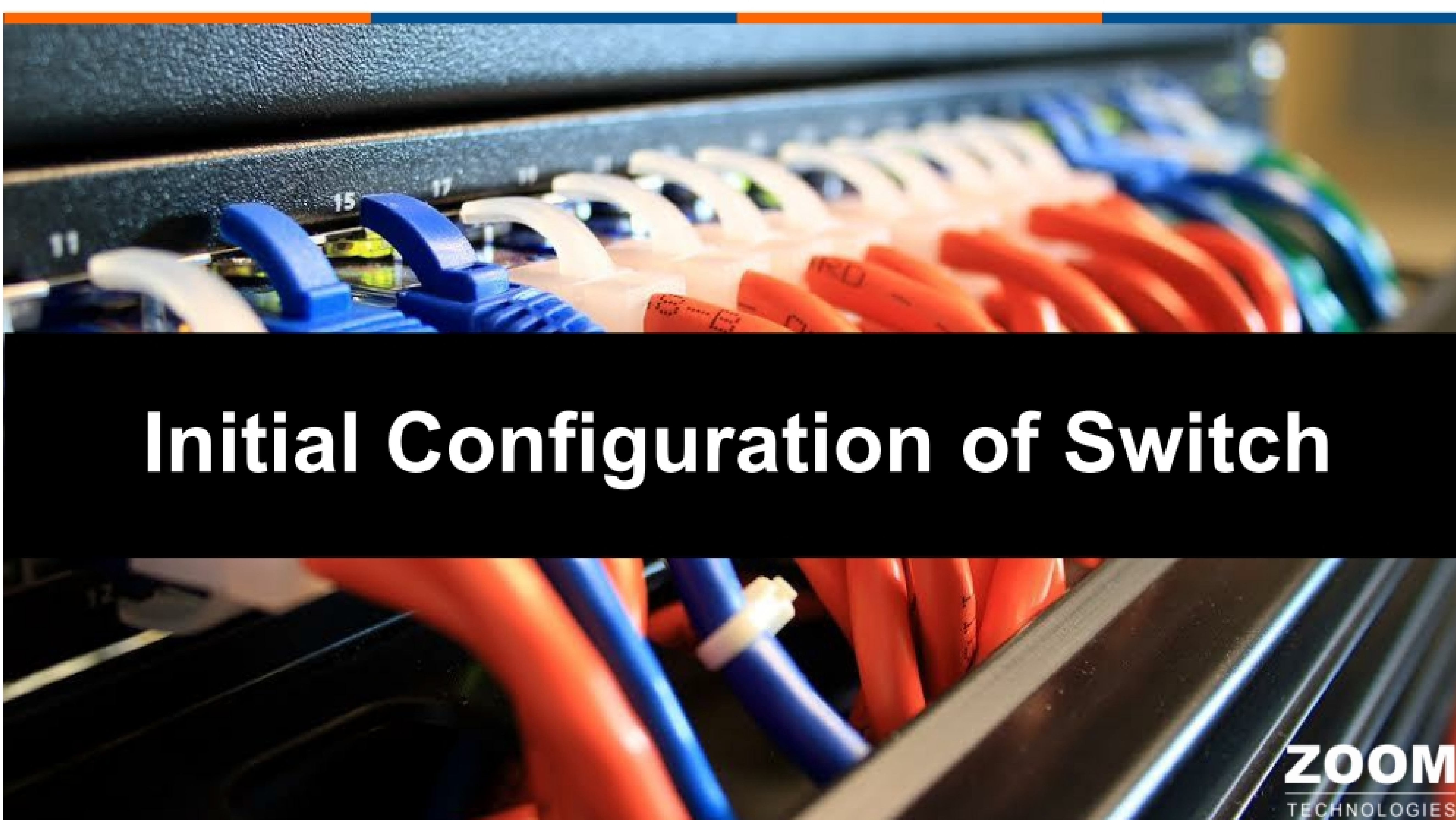


Cisco’s Hierarchical Design for switches

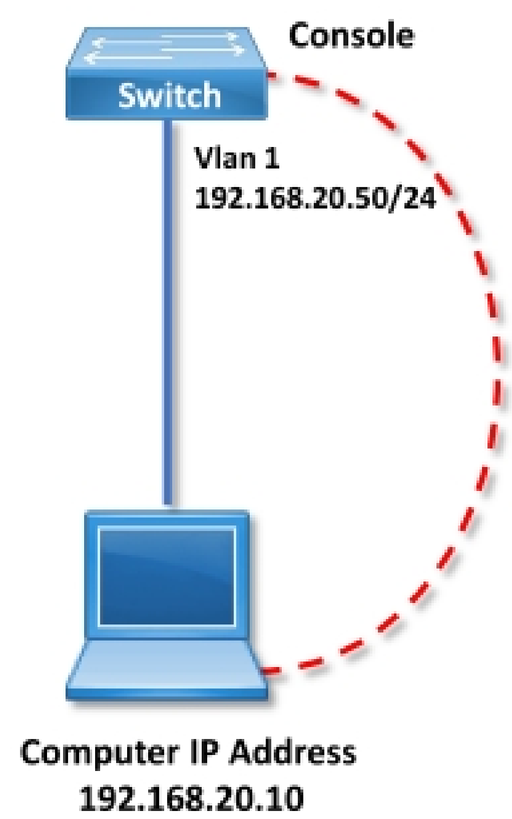
- **Access Layer Switches**
  Switches Series : 1900, 2950, 2960

- **Distribution Layer Switches**
  Switches Series :
  - **Fixed : 3550, 3560, 3750**
  - **Modular: 4500, 5500**

- **Core Layer Switches**
  Switches Series : 6500



Initial Configuration



Duplex and Speed

- Switch automatically adjusts duplex mode and speed depending upon remote device.
- We can set duplex mode and speed to match any of the supported modes.

Interface Speed & Duplex - Configuration

Switch (config) # interface < interface type > < no.>
Switch (config-if) # speed { 100 | 1000 | 10000 | auto }

Switch (config) # interface < interface type > < no.>
Switch (config-if) # duplex { full | half }

Methods of Switching

- Cisco switches supports three types of switching
  - Store and Forward
  - Cut Through
  - Fragment Free

Store and Forward

- This is basic mode of switching.
- Switch stores the entire frame into memory and perform CRC check, to ensure the frame is not corrupted.
- A frame less than 64 bytes and greater than 1518 bytes is invalid, only valid frames are processed, invalid are dropped.
- Latency is more

Cut Through

- The switch reads only the first 6bytes of frame that is destination MAC address.
- As there is no CRC check the corrupted frames are also forwarded.
- This is the fastest method of switching.
- Invalid frames are processed.

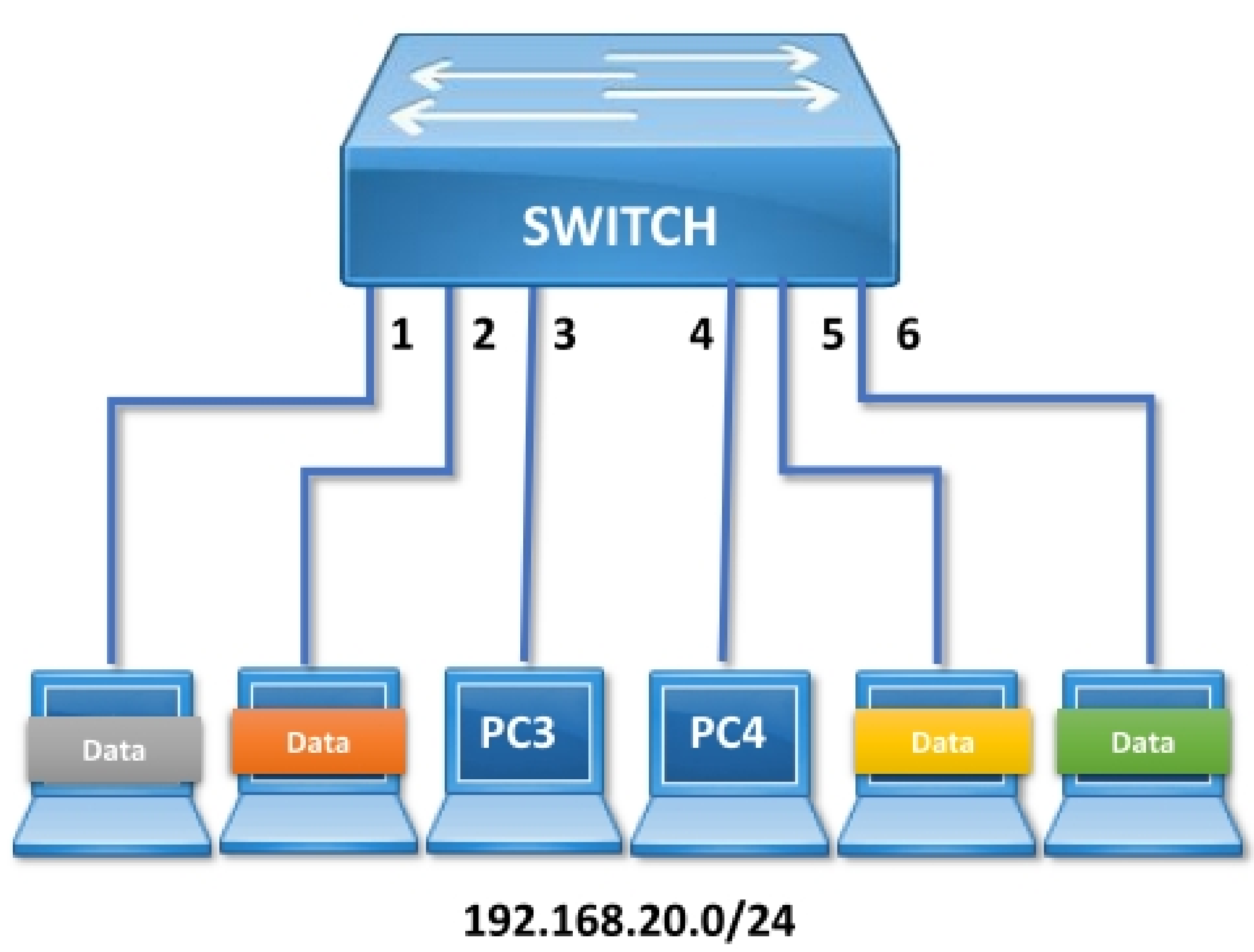
Fragment Free

- This is best method for switching.
- Switch checks only first 64bytes of frame for error.
- It processes only that frames that have first 64 bytes valid
- Any frame less than 64bytes is called as RUNT and this frame is invalid.
- Low latency.

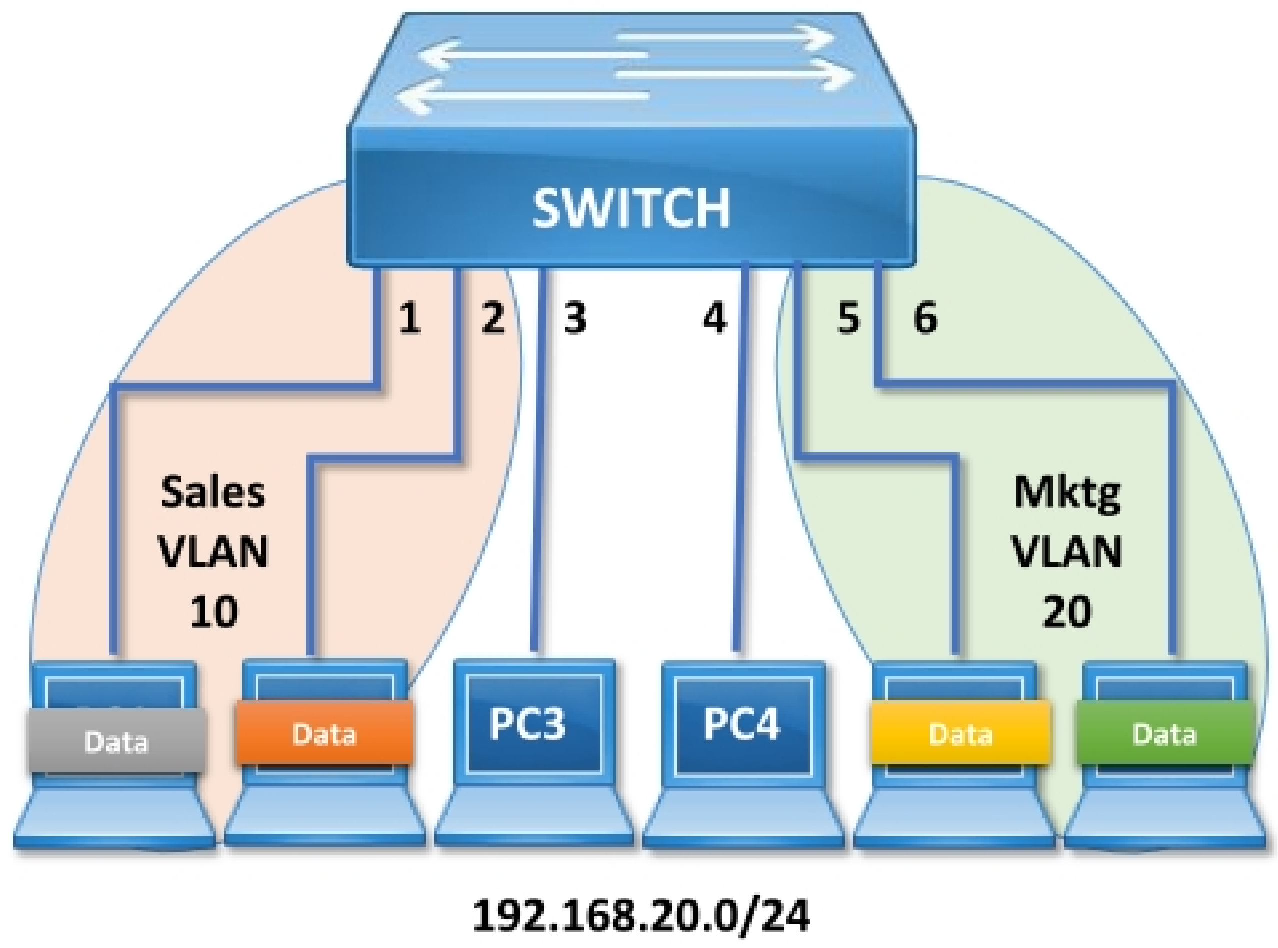
Virtual LAN

- Divides a Single Broadcast domain into Multiple Broadcast domains.
- VLANs group interfaces to create a smaller broadcast domain.
- It provides Layer 2 Security.
- By default all ports of the switch are in VLAN1.
- VLAN1 is known as Administrative VLAN or Management VLAN
- VLAN can be created from 2 – 1001.
- VLAN information is stored in vlan.dat on the flash memory of the switch.

How LAN works ?



How VLAN works ?



VLAN - Configuration

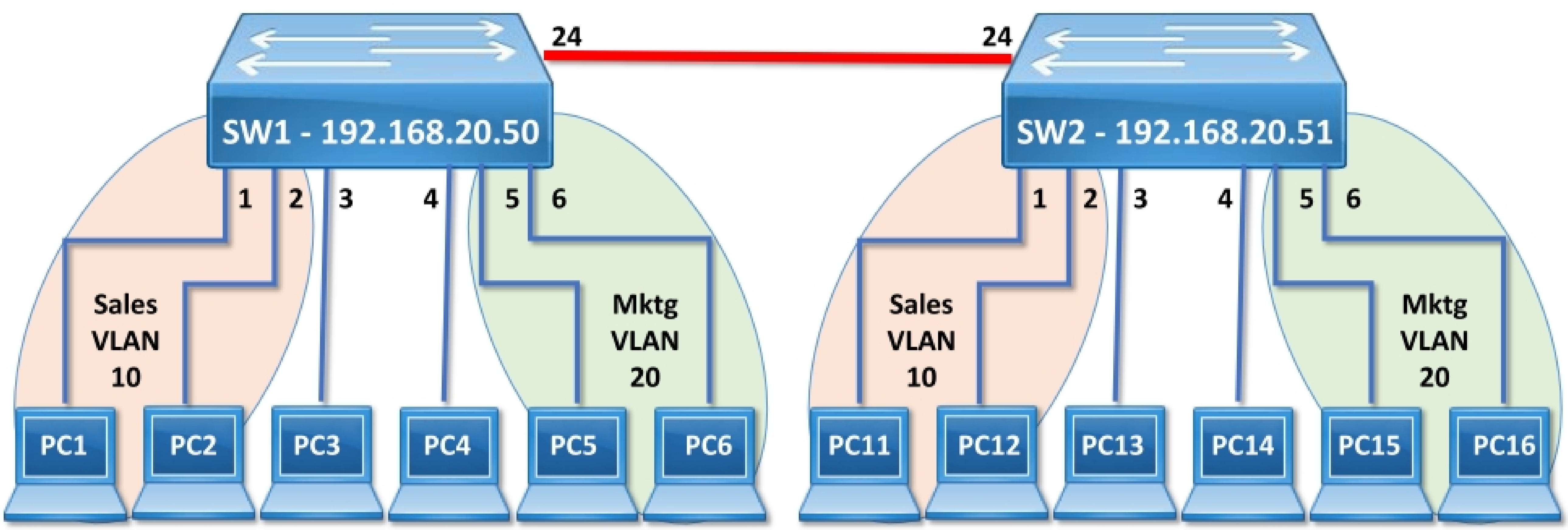
Creating VLAN

Switch (config) # vlan < vlan number >
Switch (config-vlan) # name < name >
Switch (config-vlan) # exit

Implementation of Vlan

Switch (config) # interface <interface type> <interface no>
Switch (config-if) # switchport mode access
Switch (config-if) # switchport access vlan < Vlan ID >
Switch (config-if) # exit

VLAN - Configuration



VLAN - Configuration

SW1

SW1 (config) # vlan 10
SW1 (config-vlan) # name SALES
SW1 (config-vlan) #exit
SW1 (config) # vlan 20
SW1 (config-vlan) # name MKTG
SW1 (config-vlan) #exit
SW1 (config) # interface range fastethernet 0/1 -2
SW1 (config-if-range) # switchport mode access
SW1 (config-if-range) # switchport access vlan 10
SW1 (config-if-range) # exit
SW1(config) #
SW1 (config) # interface range fastethernet 0/5 -6
SW1 (config-if-range) # switchport mode access
SW1 (config-if-range) # switchport access vlan 20
SW1 (config-if-range) # exit

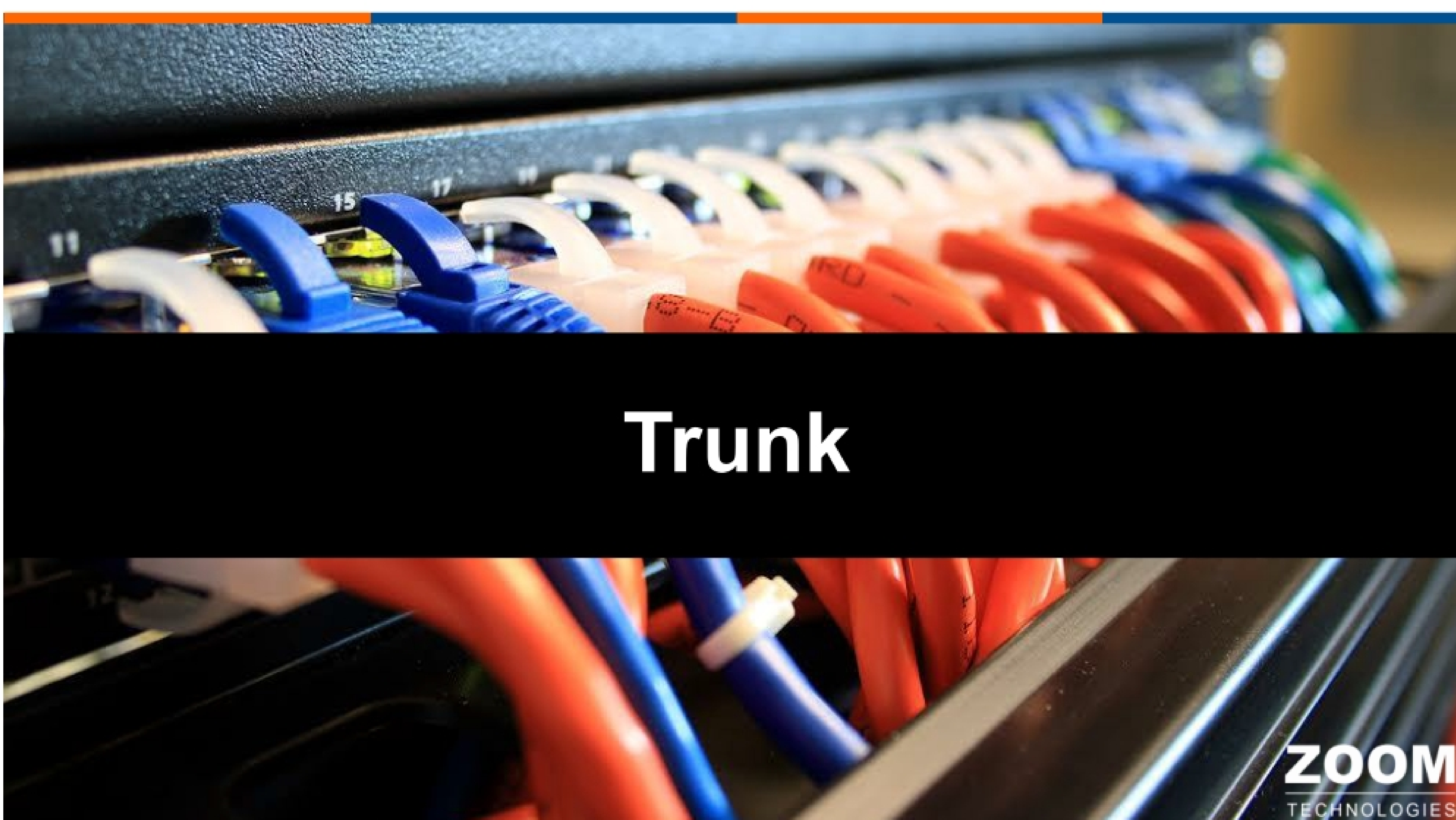
SW2

SW2 (config) # vlan 10
SW2 (config-vlan) # name SALES
SW2 (config-vlan) #exit
SW2 (config) # vlan 20
SW2 (config-vlan) # name MKTG
SW2 (config-vlan) #exit
SW2 (config) # interface range fastethernet 0/1 -2
SW2 (config-if-range) # switchport mode access
SW2 (config-if-range) # switchport access vlan 10
SW2 (config-if-range) # exit
SW2(config) #
SW2 (config) # interface range fastethernet 0/5 -6
SW2 (config-if-range) # switchport mode access
SW2 (config-if-range) # switchport access vlan 20
SW2 (config-if-range) # exit

VLAN – Verification

Switch # show vlan

Switch # show interface <interface type> <interface no.> switchport



Trunk

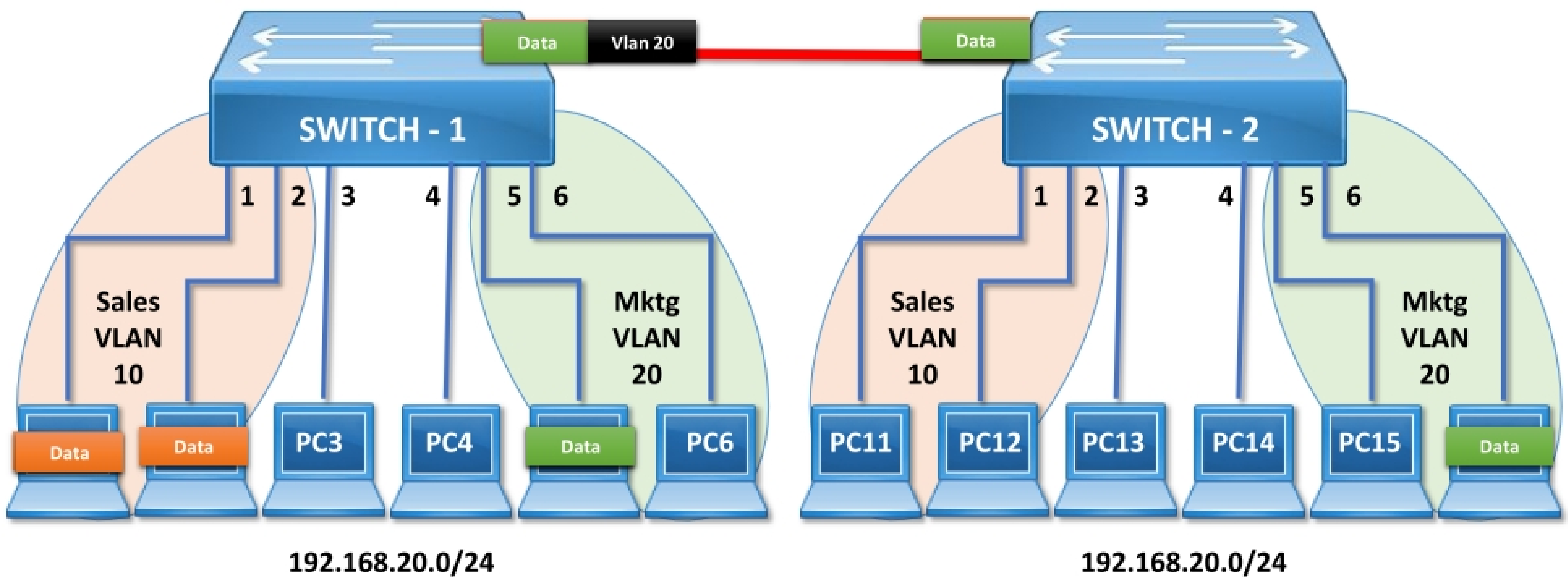
- Trunk Port allows multiple VLAN traffic to pass through a single physical connection by adding a header to Ethernet frame.
- Trunking protocols of two different types

ISL (Inter Switch Link)	802.1q
Cisco proprietary	Open standard
30 bytes (Header + Trailer)	4 bytes (Header)

VLAN Tagging

- VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.
- Each frame has a tag that specifies the VLAN it belongs to.
- Tag is added to the frame when it goes on to the trunk and tag is removed when it leaves the trunk.
- Switch forwards the frame to a particular VLAN based on tag information.

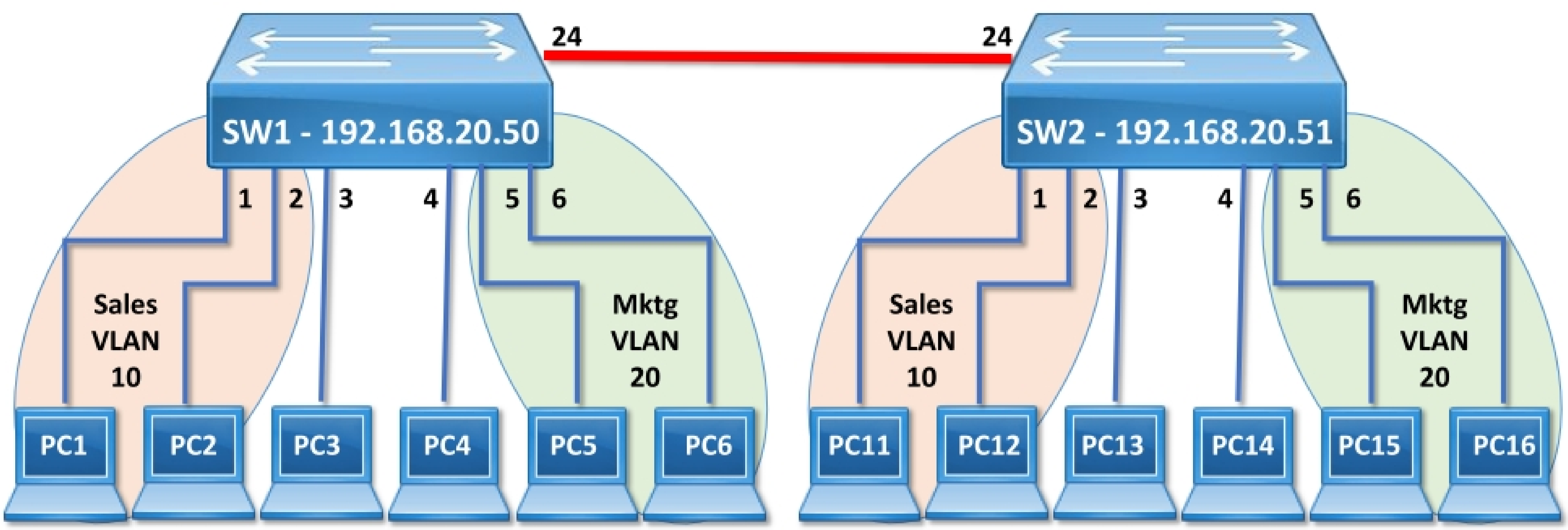
How VLAN Tagging works ?



Trunk - Configuration

Switch (config) # interface <interface type> <interface no.>
Switch (config-if) # switchport mode trunk
Switch (config-if) # switchport trunk allowed vlan <vlan id / all>
Switch (config-if) # end

Trunk - Configuration



Trunk - Configuration

SW1

```
SW1 (config)# interface fastethernet 0/24
SW1 (config-if)# switchport mode trunk
SW1 (config-if)# switchport trunk allowed vlan all
SW1 (config-if)# ^Z
SW1 #
```

SW2

```
SW2 (config)# interface fastethernet 0/24
SW2 (config-if)# switchport mode trunk
SW2 (config-if)# switchport trunk allowed vlan all
SW2 (config-if)# ^Z
SW2 #
```

Trunk – Verification

Switch # show interface trunk

Switch # show interface <interface type> <interface no.> switchport

Native VLAN

- The native VLAN is the only VLAN whose frames are not tagged on a trunk, i.e. native VLAN frames are transmitted unchanged.
- By default VLAN 1 is native VLAN, we can however configure another VLAN as native VLAN.

Native VLAN - Configuration

Switch (config) # interface <interface type> <interface no.>
Switch (config-if) # switchport trunk native vlan <vlan id>
Switch (config-if) # end

Native VLAN – Verification

Switch # show interface trunk

Dynamic Trunking Protocol (DTP)

- DTP is a Cisco proprietary protocol.
- DTP is responsible for dynamically negotiates trunks between Switches.
- DTP is enabled in all Cisco switches by default.
- DTP modes
  - Dynamic desirable
  - Dynamic auto

DTP Modes

Command Option	Description
Access	Always act as an access (Non-Trunk) port
Trunk	Always act as a Trunk port
Dynamic Desirable	Initiates negotiation messages and responds to negotiation messages to start using Trunking
Dynamic Auto	Passively waits to receive trunk negotiation messages

DTP Modes

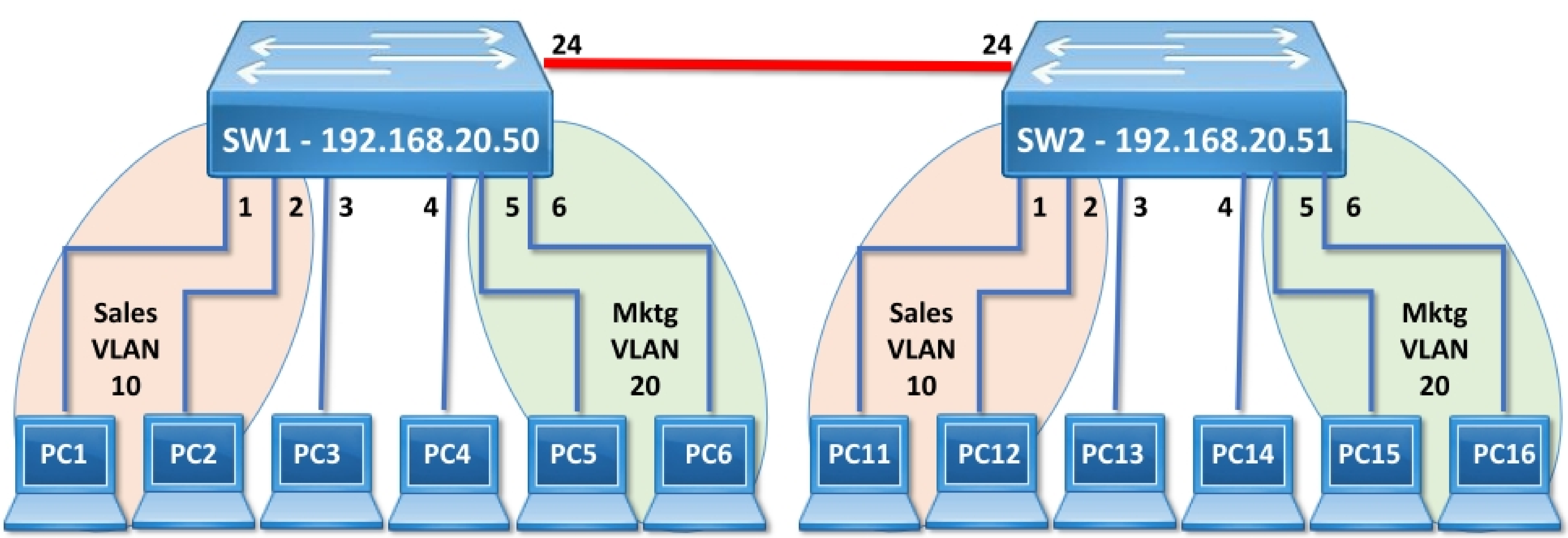
DTP - Configuration

Switch (config) # interface <interface type> <interface no.>

Switch (config-if) # switchport mode { dynamic auto | dynamic desirable}

Switch (config-if) # end

DTP - Configuration



DTP - Configuration

SW1 (config)# interface fastethernet 0/24
SW1 (config-if)# switchport mode dynamic desirable
SW1 (config-if)# end
SW1 #

SW2 (config)# interface fastethernet 0/24
SW2 (config-if)# switchport mode dynamic auto
SW2 (config-if)# end
SW2 #

DTP – Verification

Switch # show interface trunk

Switch # show interface <interface type> <interface no.> switchport

VLAN Trunking Protocol (VTP)

ZOOM TECHNOLOGIES

- **Cisco proprietary protocol created to maintain VLAN configuration consistency throughout the network.**
- **It provides accurate VLAN tracking and monitoring.**
- **Dynamic reporting of added VLANs.**
- **"Plug-and-play" configuration when adding new VLANs.**
- **VTP only works when trunking is configured on FastEthernet or higher ports.**

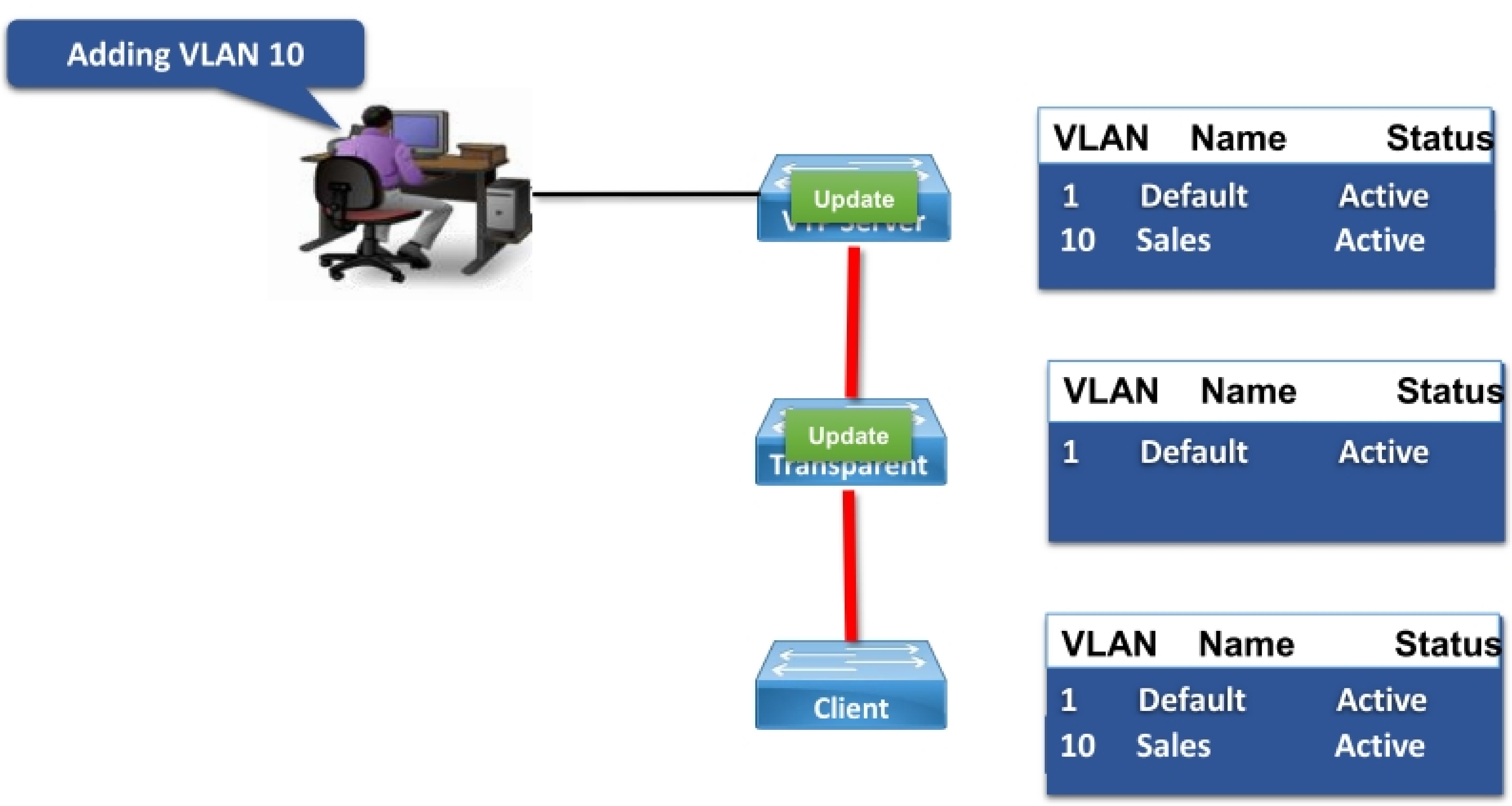
Note: Switches should be configured with same Domain Name. Domain Names are Case sensitive

CCIE CCNP CCNA

VTP Modes

- Server
  - Default mode
  - Create , Modify and Delete VLANs
  - Forwards advertisements
  - Synchronizes
- Client
  - Cannot create, Modify or delete VLANs
  - Does not store VLAN Information in the NVRAM
  - Forwards advertisements
  - Synchronizes
- Transparent
  - Create ,Modify and Delete local VLANs only
  - Forwards advertisements
  - Does not synchronize

How VTP works ?



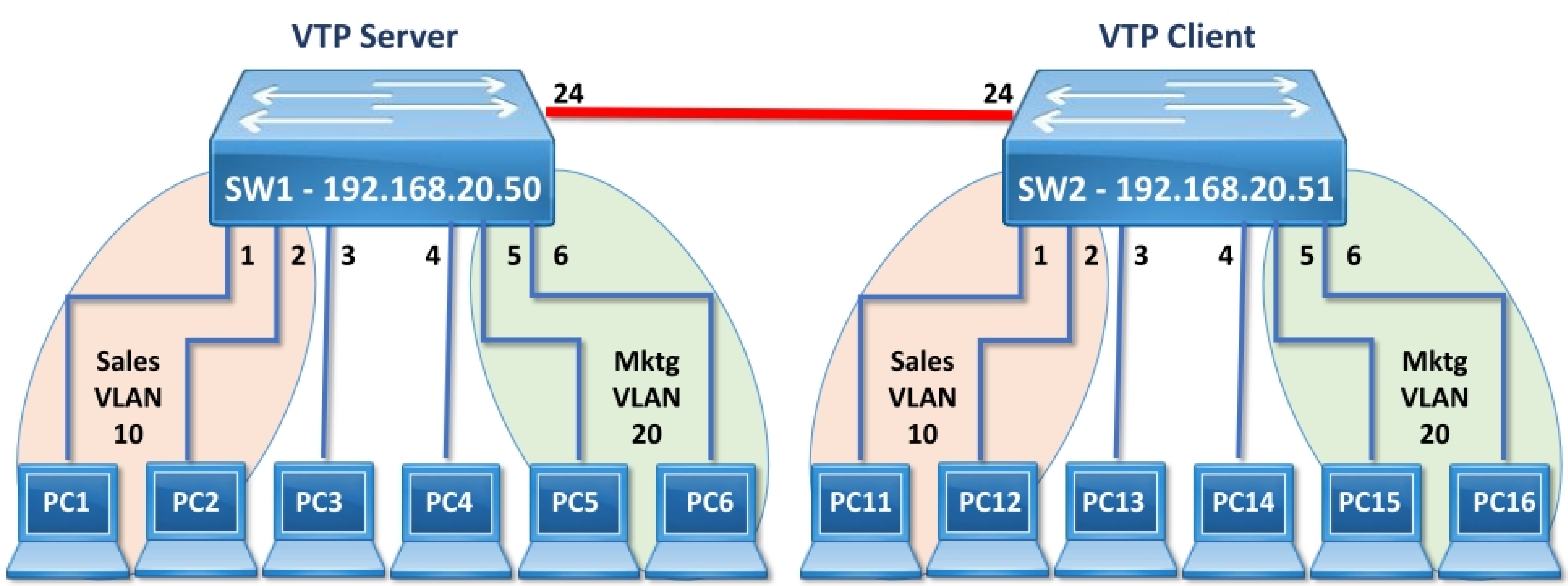
VTP - Configuration

Switch (config) # vtp mode { server | client | transparent }

Switch (config) # vtp domain < name >

Switch (config) # vtp password < password >

VTP - Configuration



VTP - Configuration

SW1

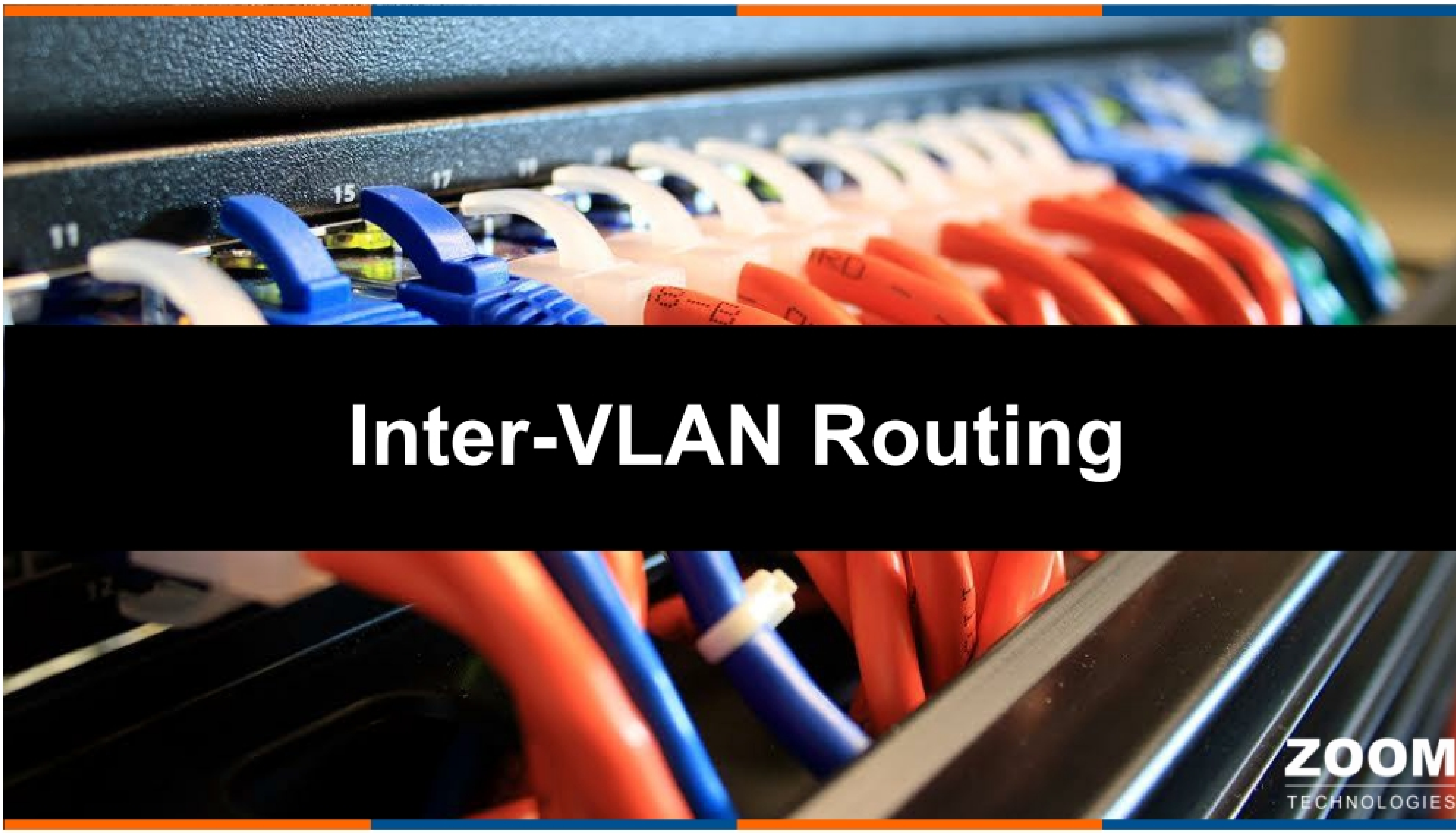
SW1 (config) # vtp domain ZOOM
Changing VTP domain name from null to ZOOM
SW1 (config) # vtp password CCNA
Setting device VLAN database password to CCNA
SW1 (config) # end
SW1 #

SW2

SW2 (config) # vtp domain ZOOM
Changing VTP domain name from null to ZOOM
SW2 (config) # vtp password CCNA
Setting device VLAN database password to CCNA
SW2 (config) # vtp mode client
Setting device to VTP CLIENT mode.
SW2 (config) # end
SW2 #

VTP – Verification

Switch # show vtp status
Switch # show vtp password



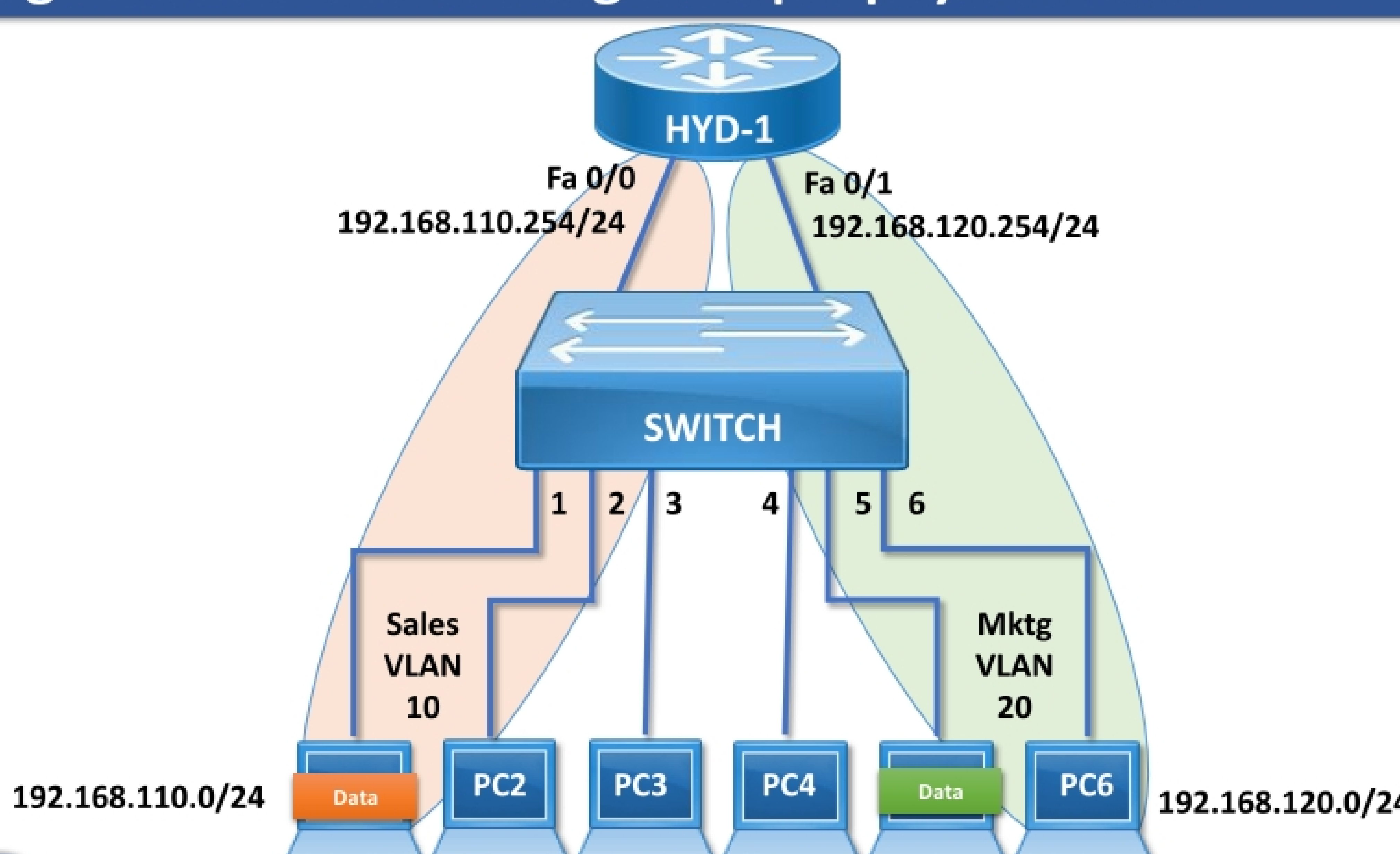
Inter-VLAN Routing

- Inter-vlan routing is a process of forwarding the traffic from one vlan to other vlan using a router.
- The port where the router is connected on switch should be configured as trunk to allow multiple vlan traffic
- The physical interface on router is divided into multiple sub-interfaces
- Each sub-interface is associated with one VLAN and one IP subnet.
- This is also called as Router on a stick.

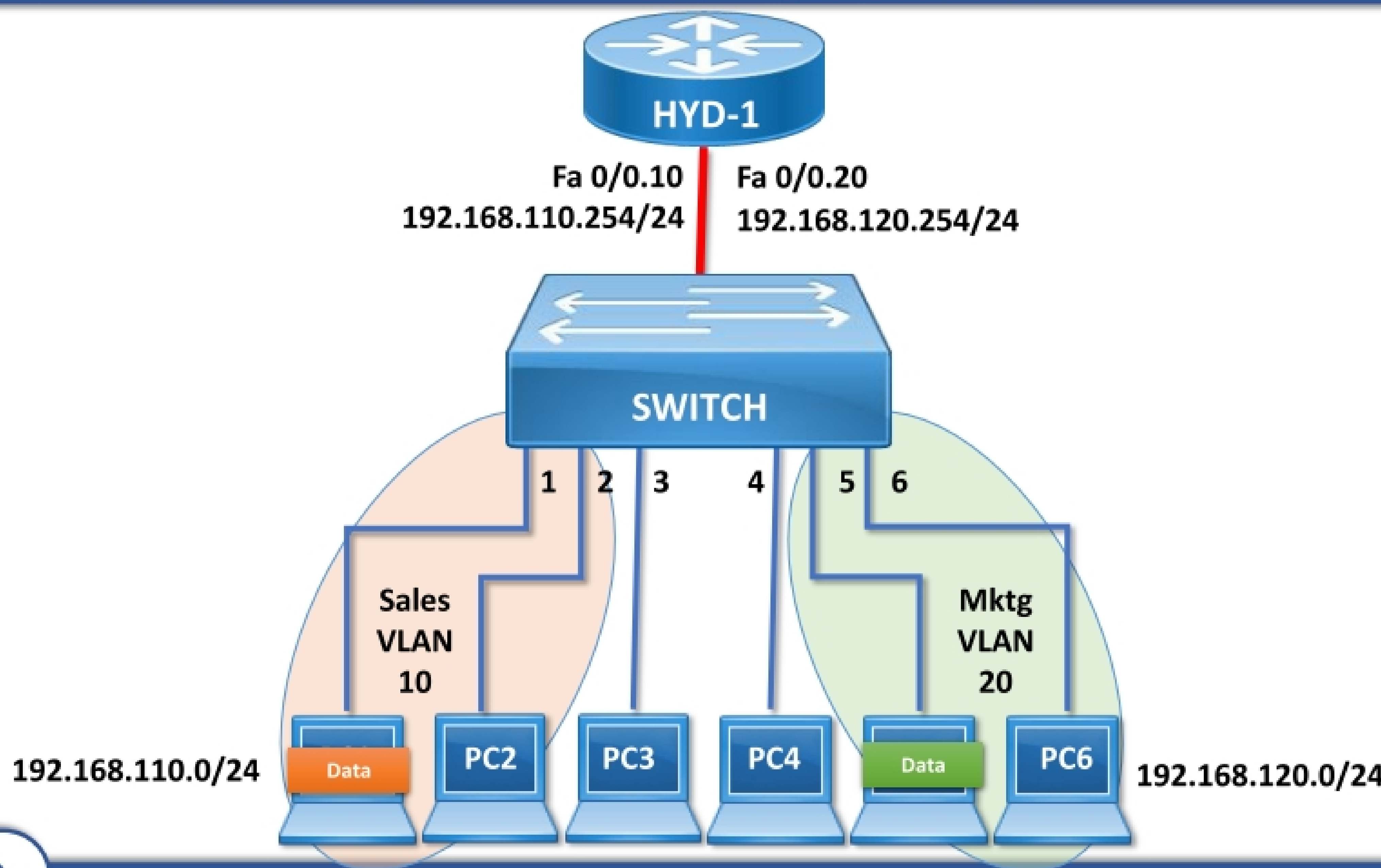
Routing between VLANs

- **Routing between VLANs can be done in below ways:**
  - **Using multiple physical links called as legacy inter-vlan routing**
  - **Using a single link and creating sub-interfaces called as router on a stick**
  - **Using the multi layer switch.**

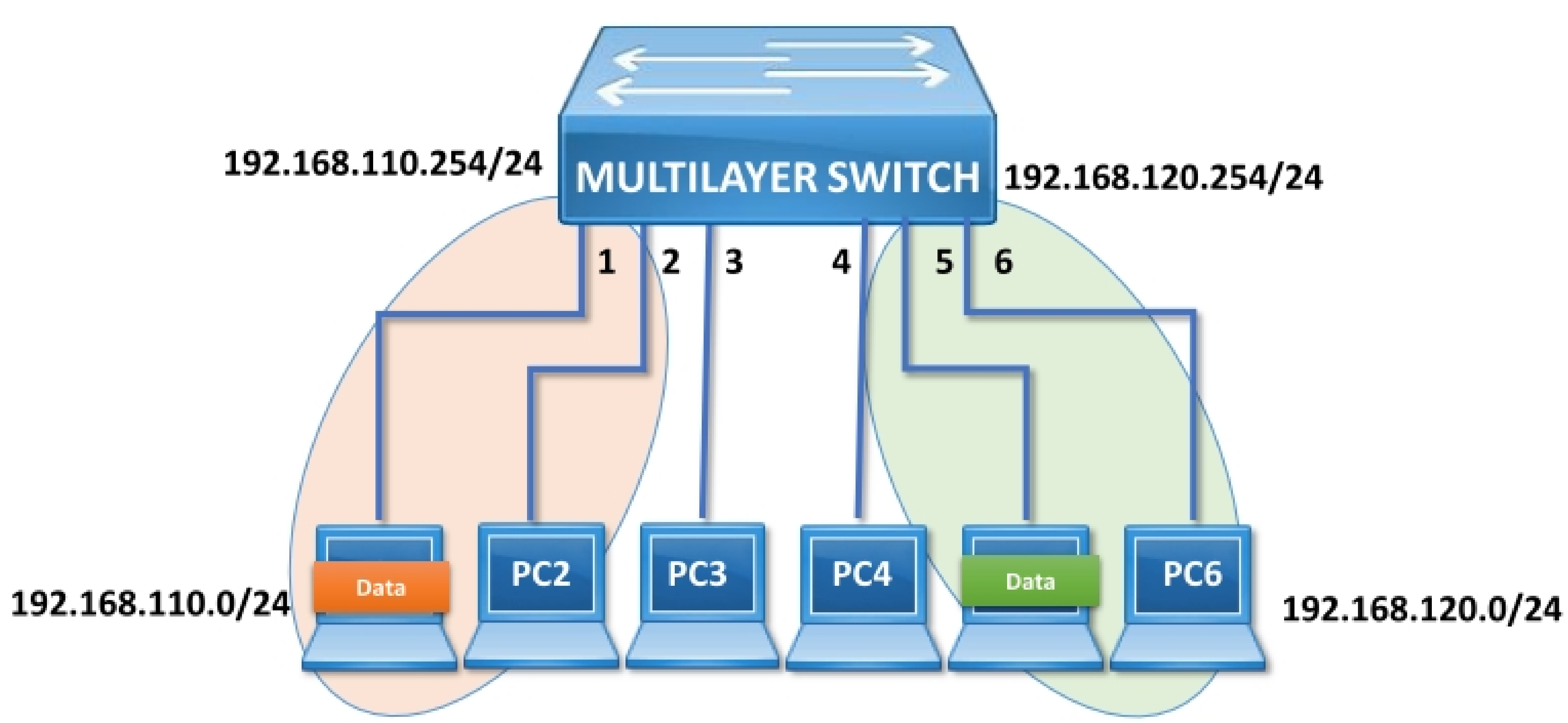
Routing between VLANs using multiple physical links



Routing between VLANs using single physical link



Routing between VLANs using Multi-layer Switch



Router on a Stick - Configuration

Creating Sub Interface

Router (config) # interface FastEthernet 0/0 . < no. >

Router (config-subif) # encapsulation dot1q < vlan id >

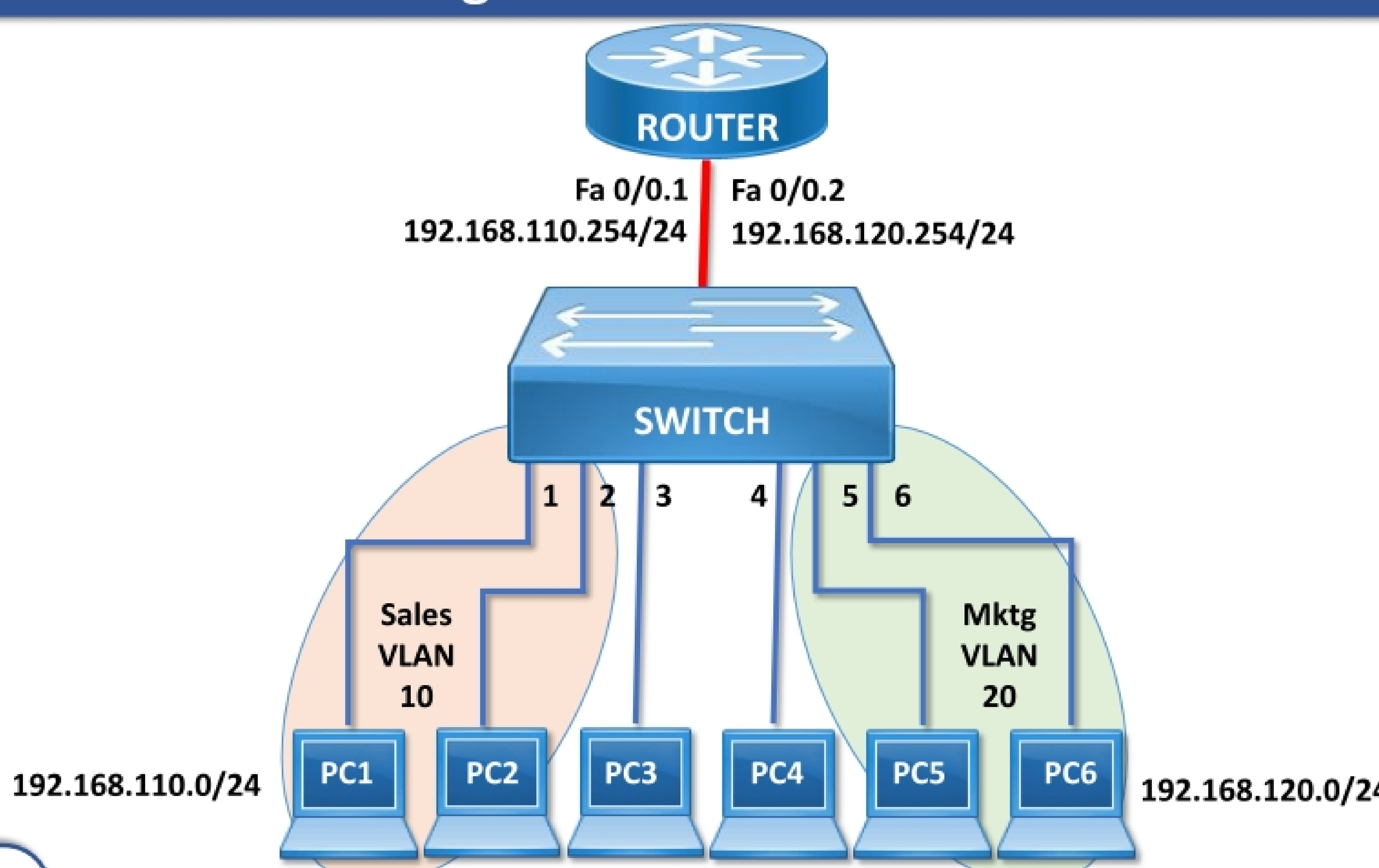
Router (config-subif) # ip address < ip > < subnet mask >

Router (config-subif) # exit

Enabling IP Routing

Router (config) # ip routing

Router on a Stick - Configuration



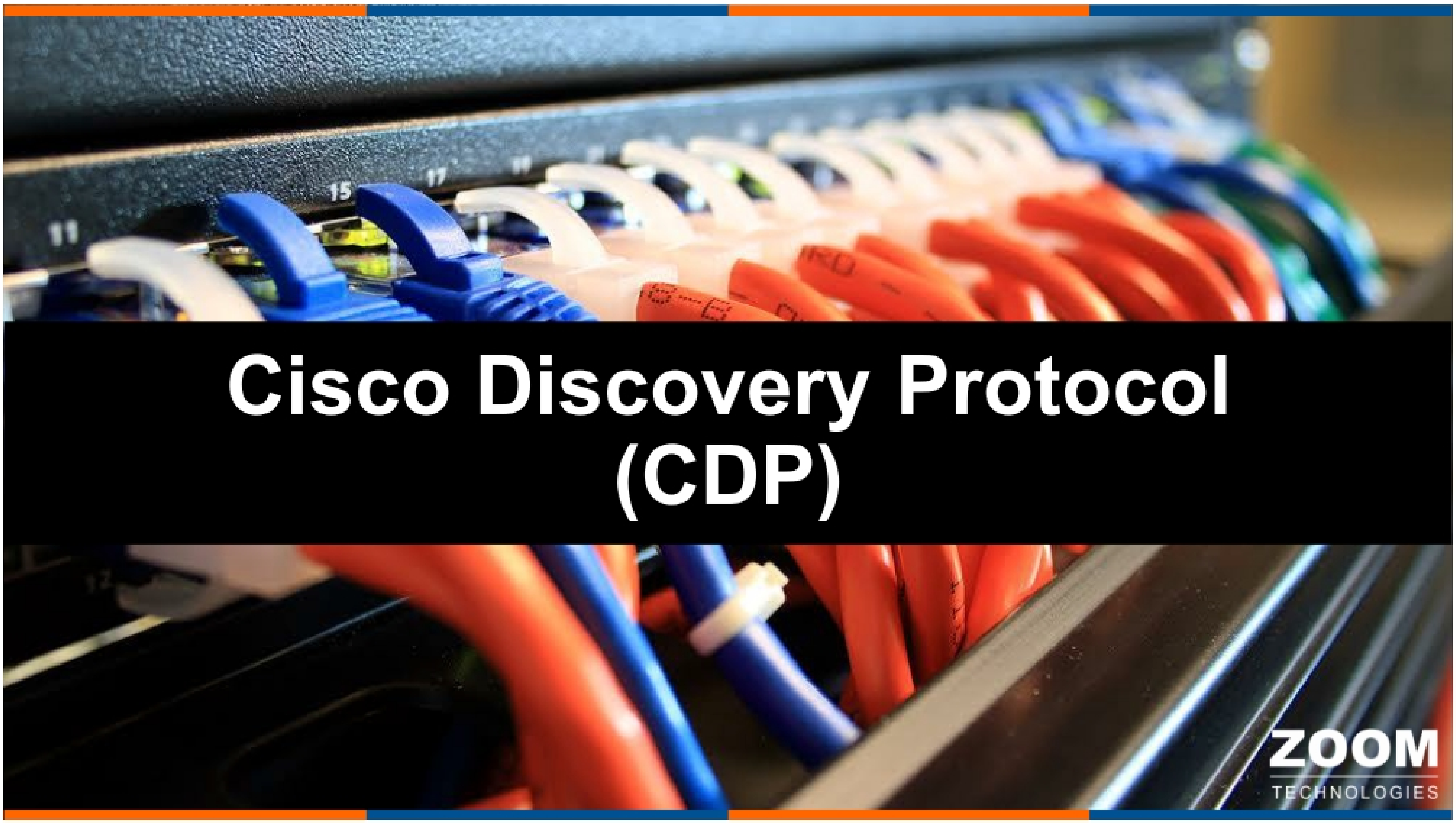
Router on a Stick - Configuration

ROUTER

```
ROUTER (config) # interface FastEthernet 0/0
ROUTER (config-if) # no shutdown
ROUTER (config-if) # exit
ROUTER (config) # interface FastEthernet 0/0.1
ROUTER (config-subif) # encapsulation dot1q 10
ROUTER (config-subif) # ip address 192.168.110.254 255.255.255.0
ROUTER (config-subif) # exit
ROUTER (config) # interface FastEthernet 0/0.2
ROUTER (config-subif) # encapsulation dot1q 20
ROUTER (config-subif) # ip address 192.168.120.254 255.255.255.0
ROUTER (config-subif) # exit
ROUTER (config) # ip routing
ROUTER (config) #
```

Router on a Stick – Verification

Router # show ip route



Cisco Discovery Protocol (CDP)

- It is a Cisco proprietary protocol.
- CDP is enabled by default in all Cisco devices.
- CDP advertisements are sent through all the ports by default.
- CDP Advertisement are sent every 60 seconds.
- CDP Advertisements are sent via multicast address 01:00:0c:cc:cc:cc.

Advantages of CDP

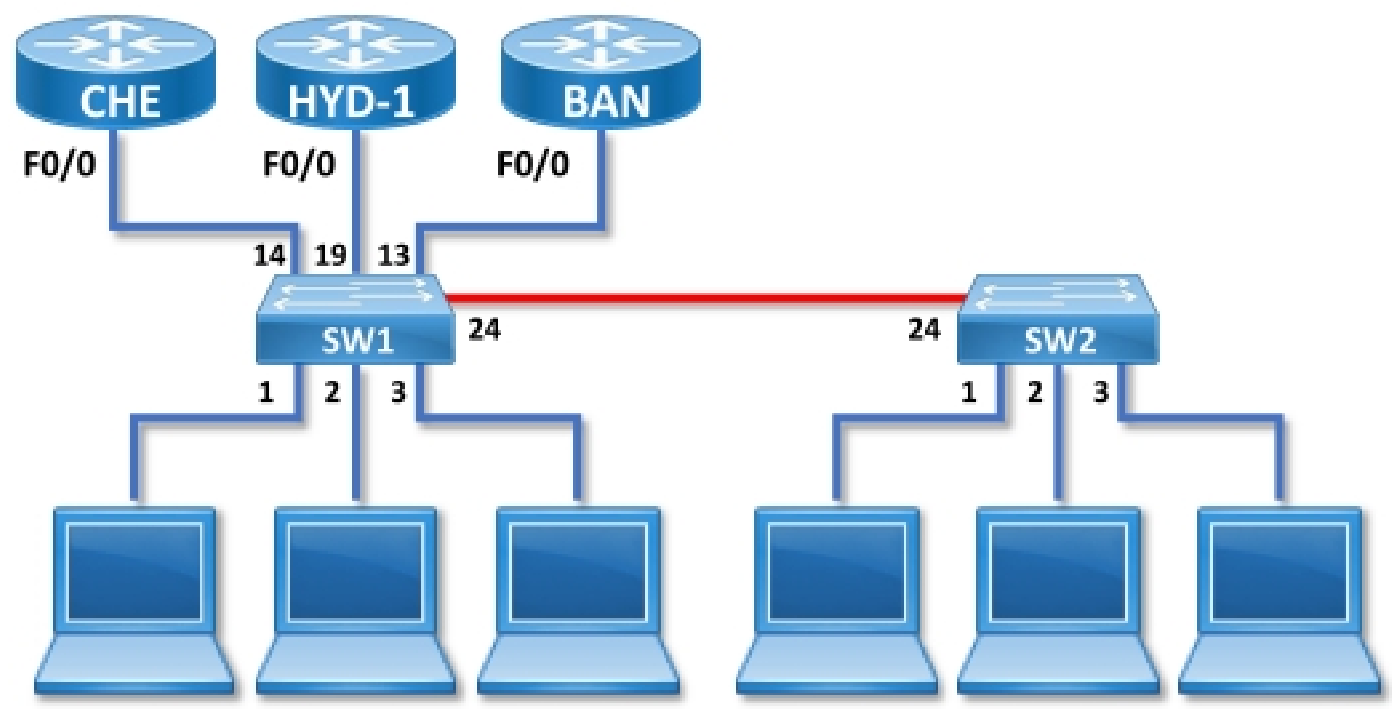
- Once Layer 1 is active CDP sends the information to its active neighbors.
- It can be used for Layer 1, Layer 2, Layer 3 troubleshooting.
- Information advertised by CDP
  - Logical address (if defined)
  - Hostname
  - Hardware Platform
  - IOS Version
  - Interface Type and Interface Number of local and remote device connected.

CDP - Configuration

Switch (config) # cdp run

CDP - Configuration

ZOOM TECHNOLOGIES



CCIE CCNP CCNA

CDP - Configuration

ZOOM TECHNOLOGIES

SW1

SW1 (config) # cdp run

SW2

SW2 (config) # cdp run

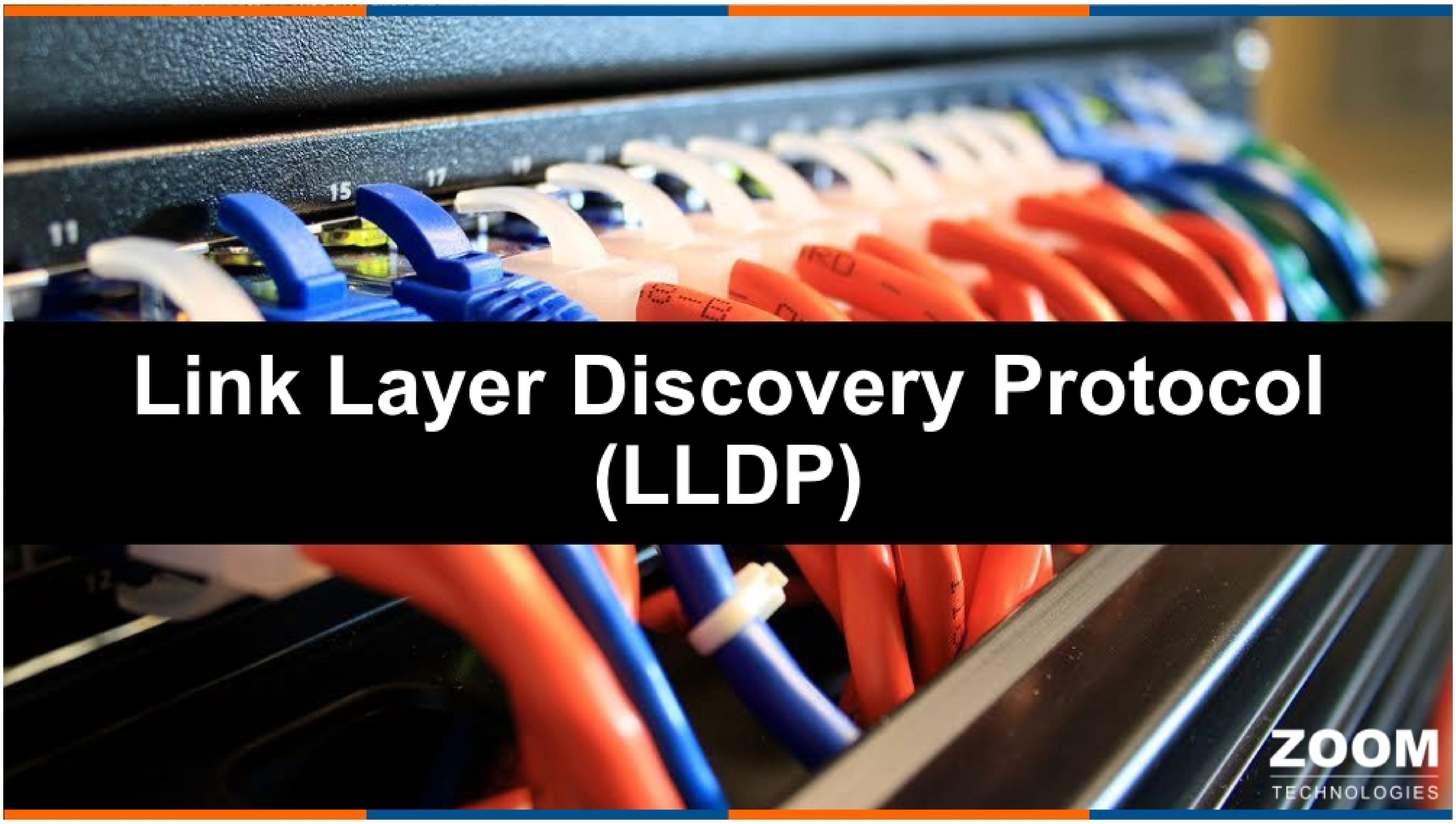
CCIE CCNP CCNA

CDP - Verification

Switch # show cdp neighbors
Switch # show cdp neighbor detail

Disadvantages Of CDP

- CDP can be used only between Cisco devices.
- Information about only directly connected neighbors can be known.



Link Layer Discovery Protocol (LLDP)

ZOOM
TECHNOLOGIES

- **Open Standard Protocol - IEEE 802.1AB**
- **LLDP is a neighbor discovery protocol used by devices for advertising information about themselves to other devices on the network.**
- **By default it is disabled on cisco devices, we need to manually enable it on devices.**
- **LLDP Advertisement are sent every 30 seconds.**
- **LLDP Advertisements are sent via multicast address 01:80:c2:00:00:0e.**

CCIE
CCNP
CCNA

LLDP - Configuration

Switch (config) # lldp run

LLDP - Verification

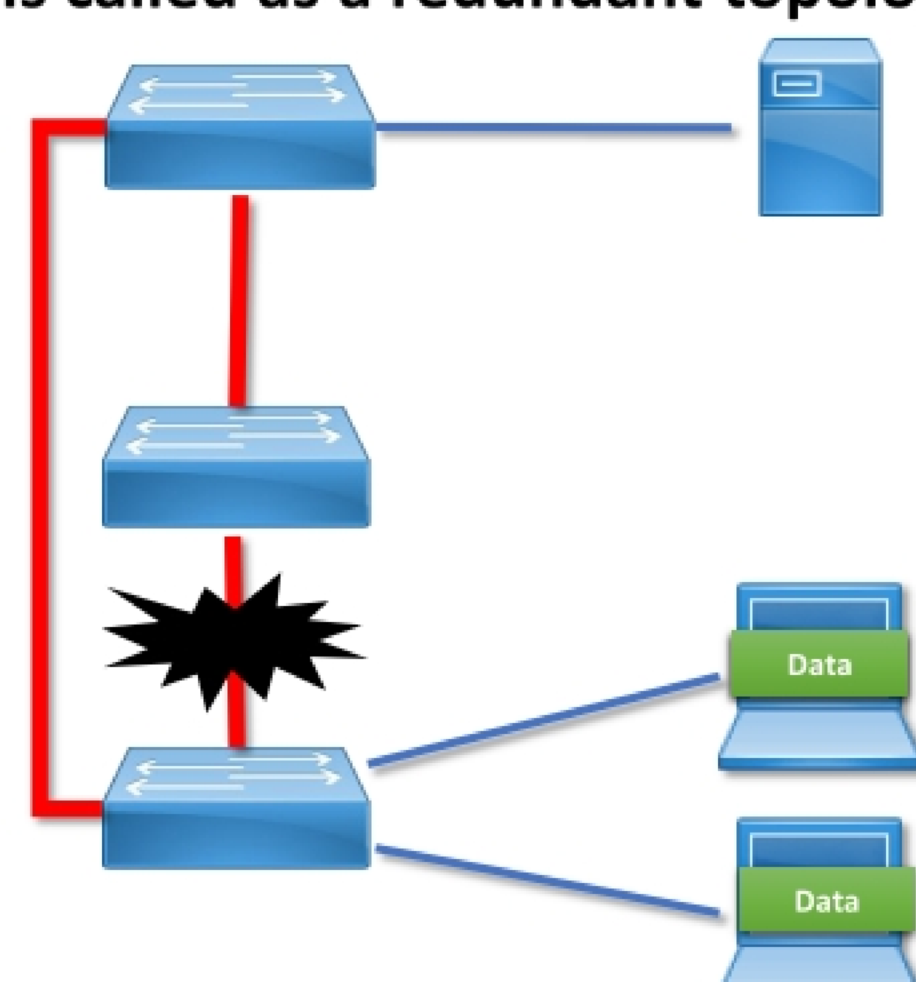
Switch # show lldp neighbors

Switch # show lldp neighbor detail

Spanning-Tree Protocol (STP)

Redundant Topology

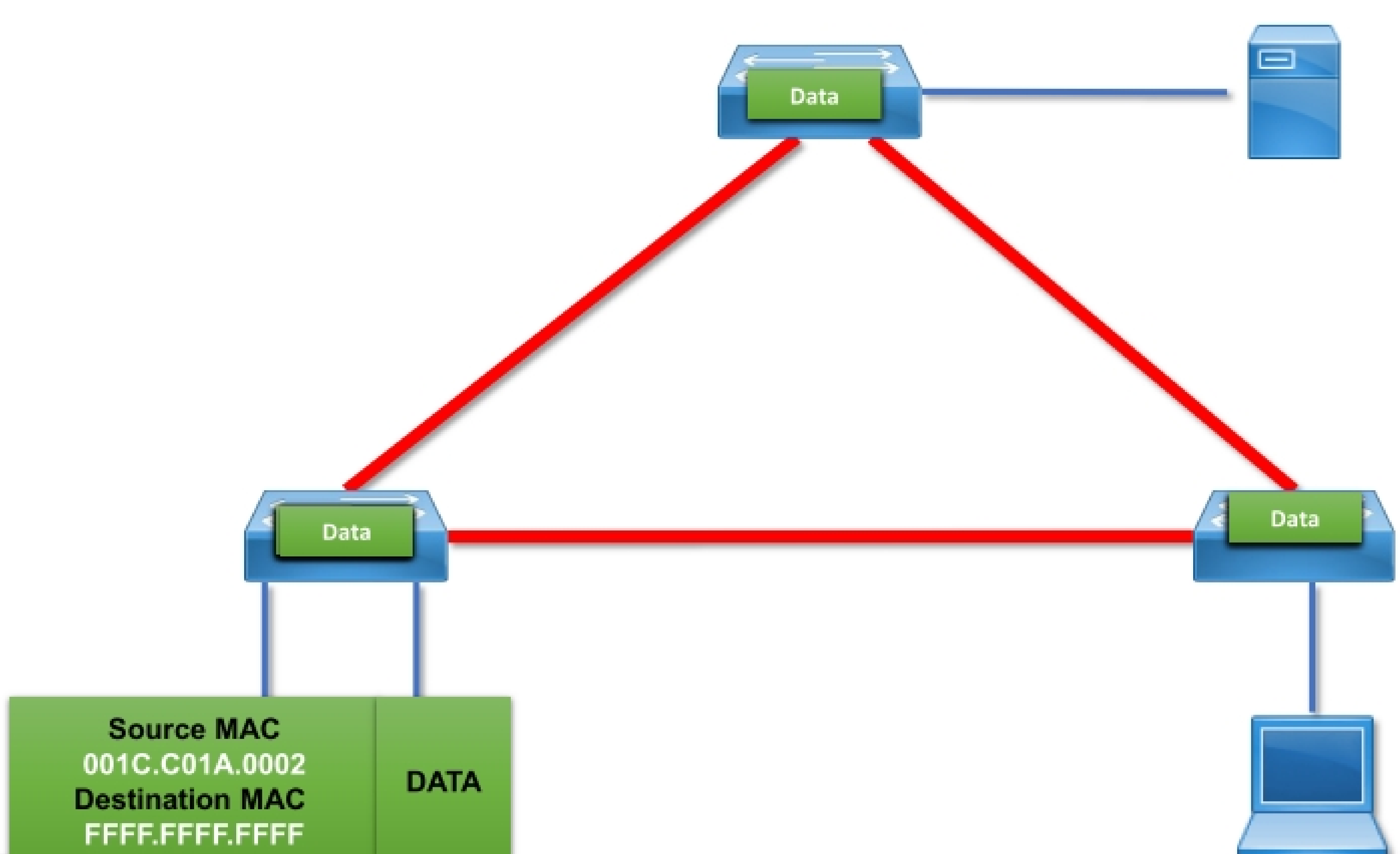
- To eliminate single point of failure, backup links are used.
- This type of network is called as a redundant topology.



Problems in Redundant Topologies

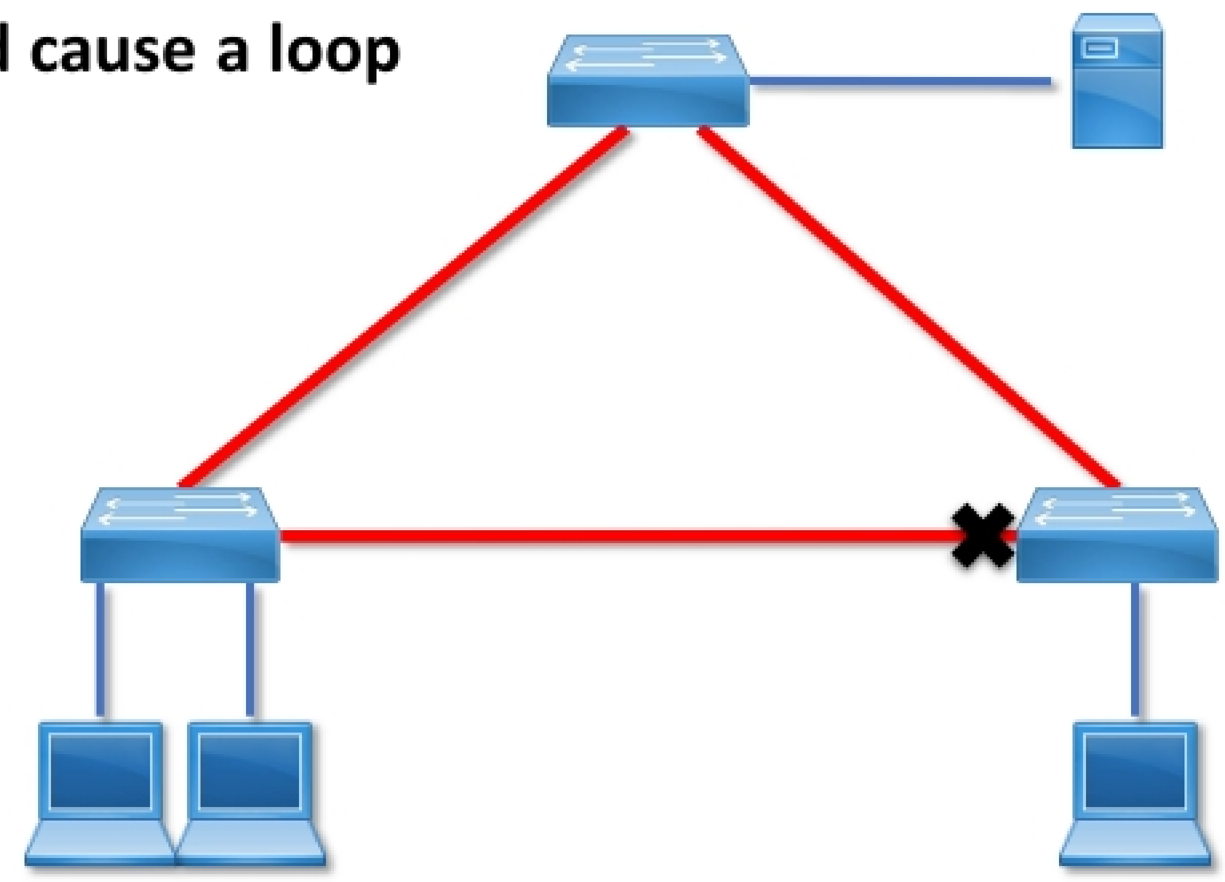
- Redundant topology causes
  - Multiple frame copies
  - MAC address table instability
  - Broadcast storms
- The above problems are collectively called layer 2 switching loops.

Problems in Redundant Topologies



Spanning-tree Protocol

- Spanning-tree protocol is used in switched network to avoid switching loops
- It uses spanning-tree algorithm
- STP blocks redundant paths that could cause a loop
- STP is a open standard (IEEE 802.1D)



STP Terminology

- Root Switch
  - The switch with the best (lowest) Switch ID.
  - Out of all the switches in the network, one switch is elected as a Root switch. This Root switch becomes the focal point of the network.
- Switch ID
  - Each switch has a unique identifier called a Bridge ID or Switch ID
  - Bridge ID = Priority + MAC address of the switch
  - Default priority is 32768
- Non-Root Switch
  - All switches other than the Root switch are called Non-root switches.

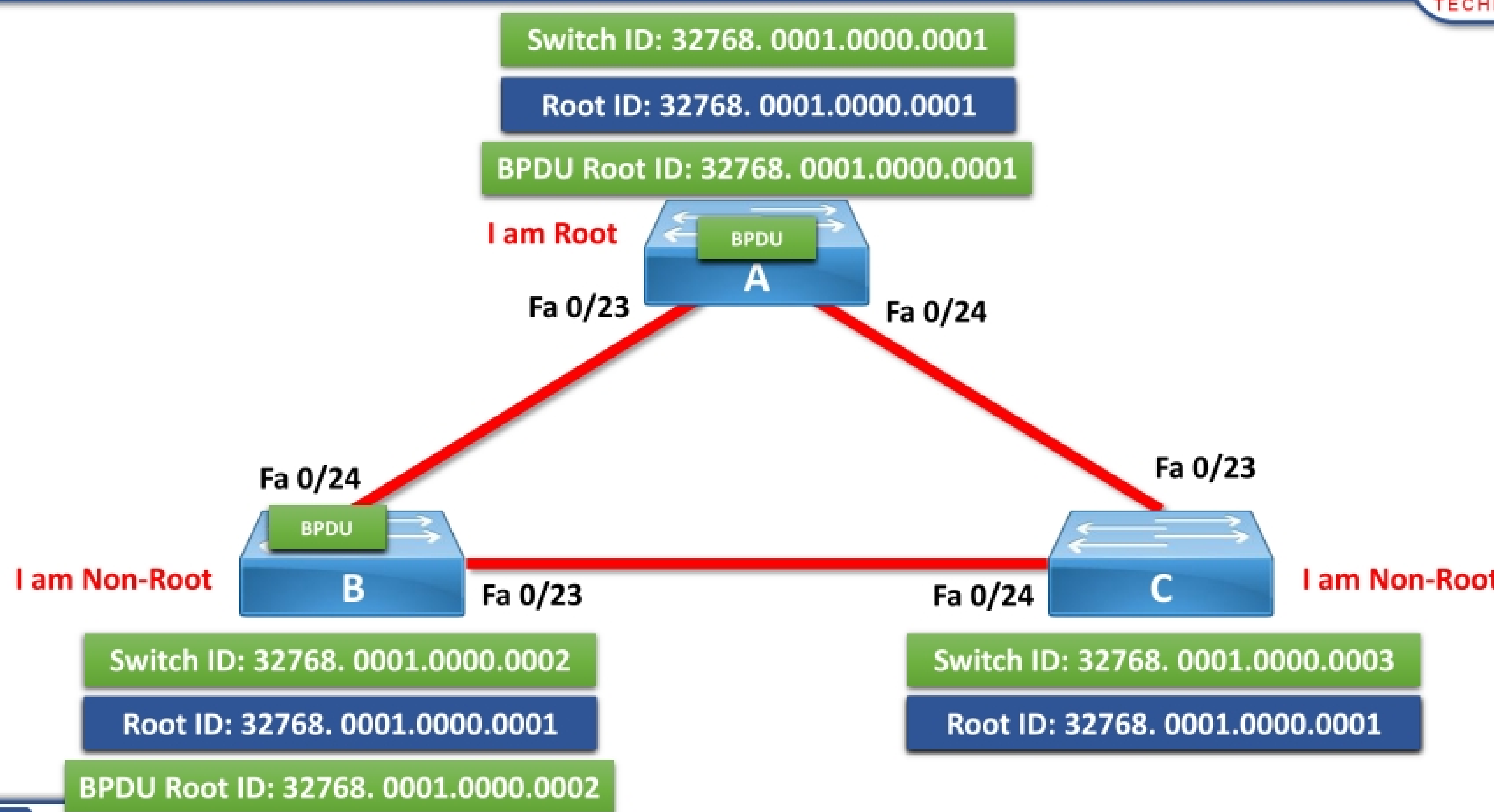
STP Terminology

- BPDU
  - Switches exchange information using Bridge Protocol Data Units (BPDUs)
  - BPDUs contain information that helps the switch to determine the topology
  - BPDUs are sent every 2 sec

STP Port states

States	Forward frames	Learn Mac-Address	BPDU	Duration
Blocking	No	No	Receives	20 seconds
Listening	No	No	Sent/receive	15 seconds
Learning	No	Yes	Sent/receive	15 seconds
Forwarding	Yes	Yes	Sent/receive	-

Root Switch Election



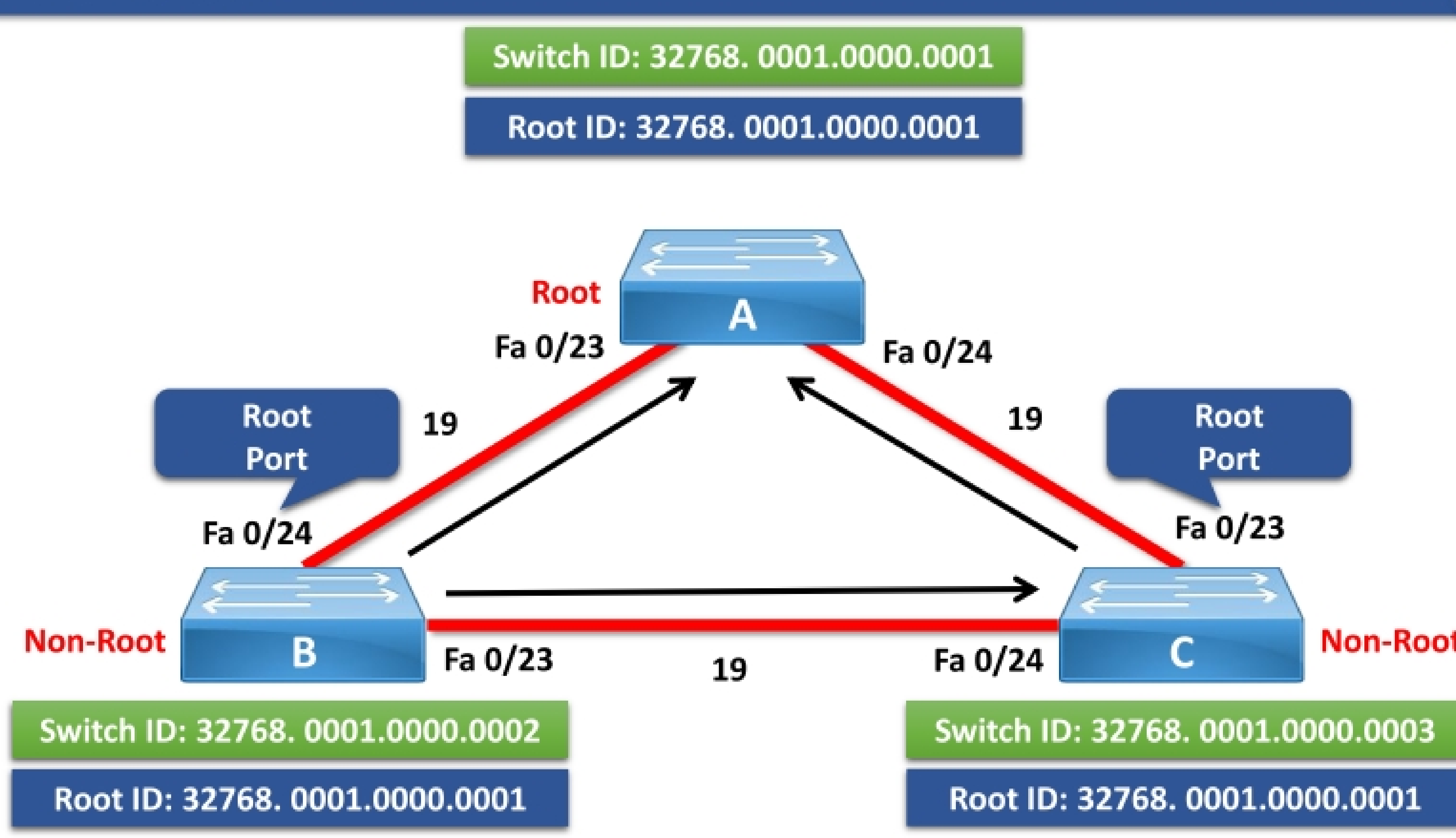
STP Terminology

- Root port
  - Every Non-Root Switch must have a Root port
  - Only one port per switch can be the Root port
  - All Root ports will be in forward state
  - A Switch's Root port is the port closest to the Root Switch
    - The port with the least cost
    - The port with the lowest Neighbor switch ID
    - Lowest Physical Port Number

IEEE Cost Values

Type	Cost Value
Ethernet	100
Fast Ethernet	19
Gigabit Ethernet	4
10 Gigabit Ethernet	2

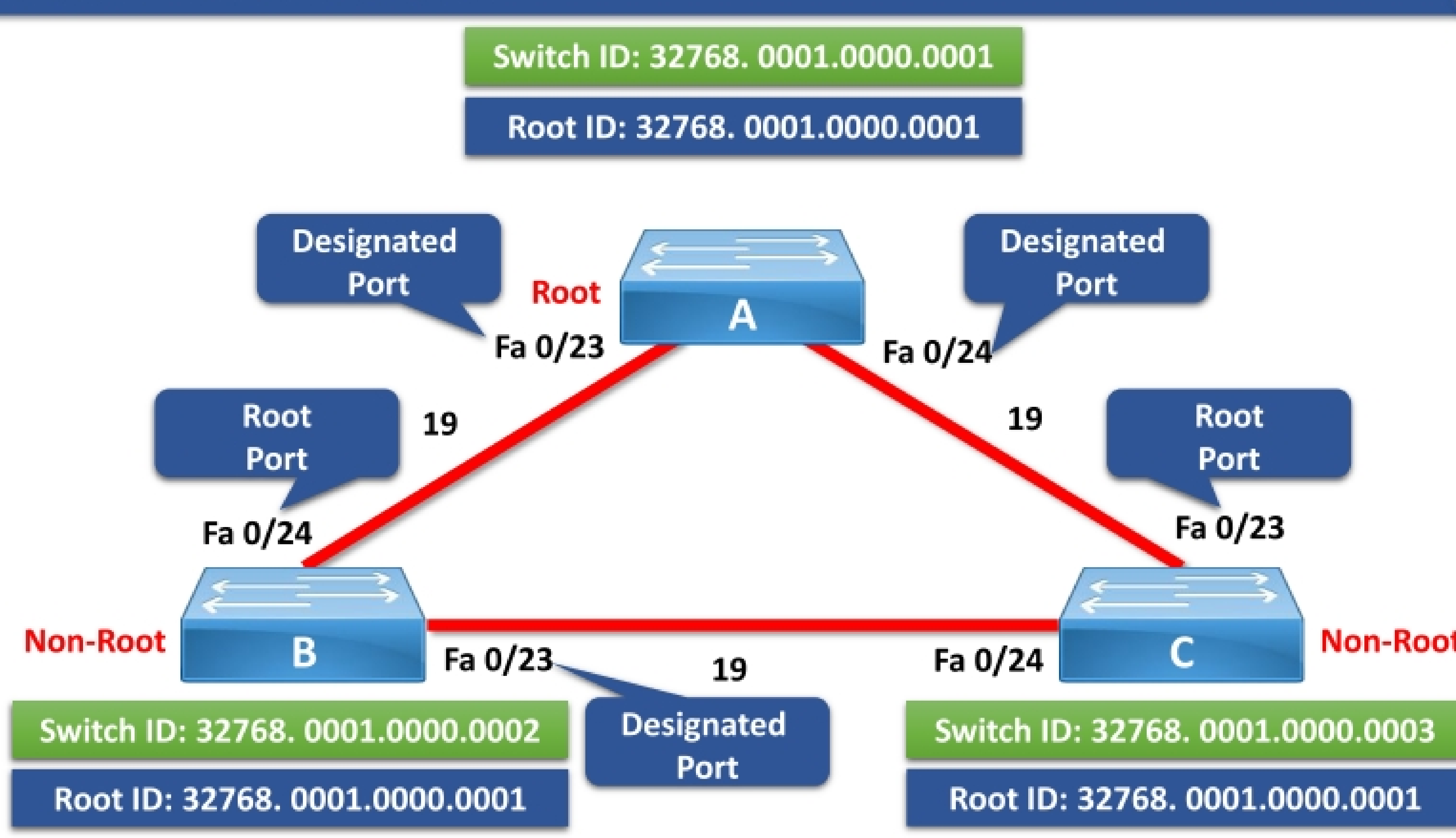
Root Port Election



Designated Port Election

- Designated port
  - For Every segment there will be a Designated port
  - A designated port will always be in Forward state
    - The port with the least cost
    - The port with the lowest Neighbor switch ID
    - Lowest Physical Port Number
  - All ports(Trunk ports) on the Root bridge are Designated ports

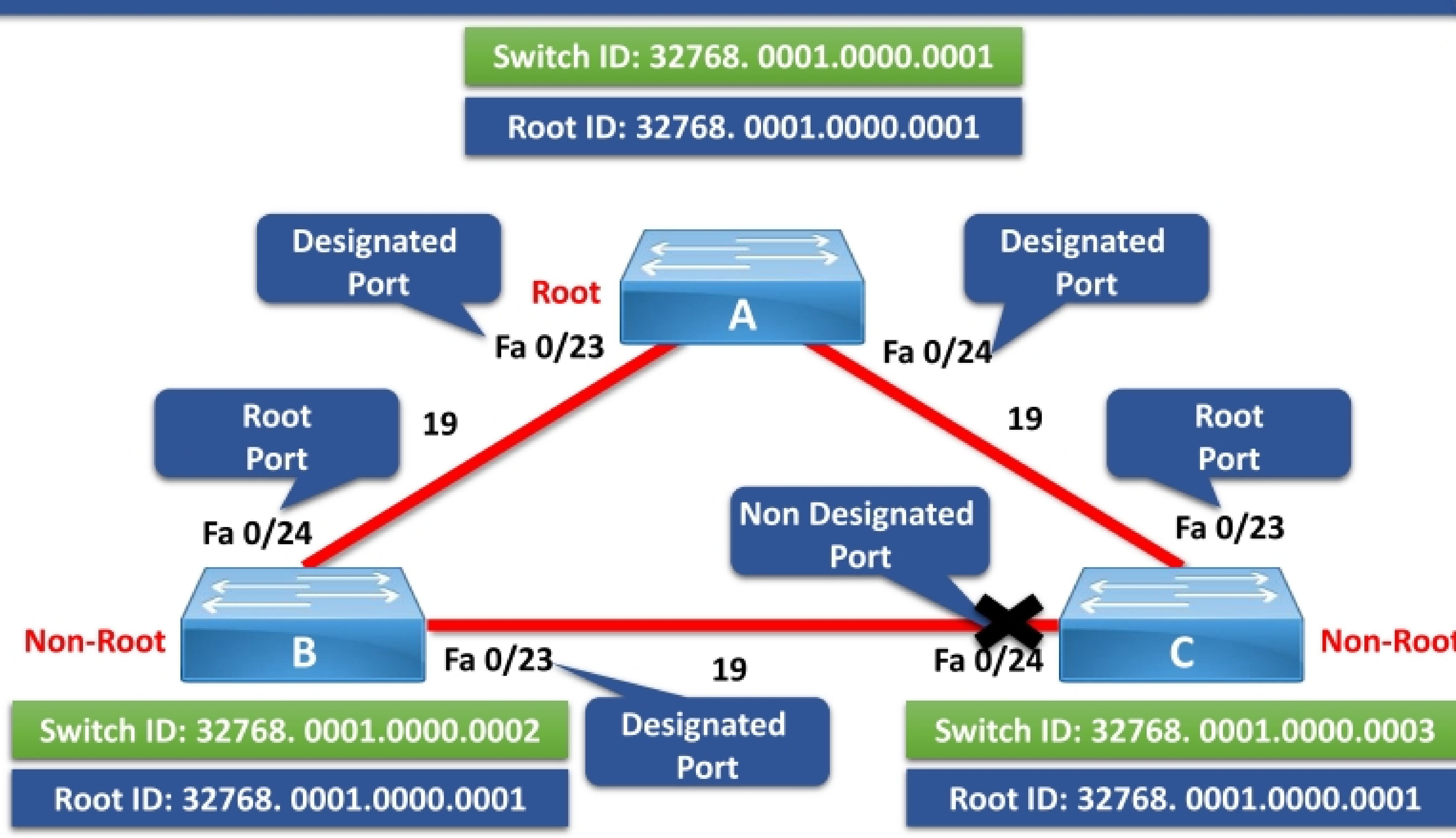
Designated Port Election



STP Terminology

- **Non-Designated port**
  - **The ports that are neither Root ports nor the Designated ports**
  - **These ports are blocked by STP**

Root Port Election



STP - Configuration

ZOOM TECHNOLOGIES

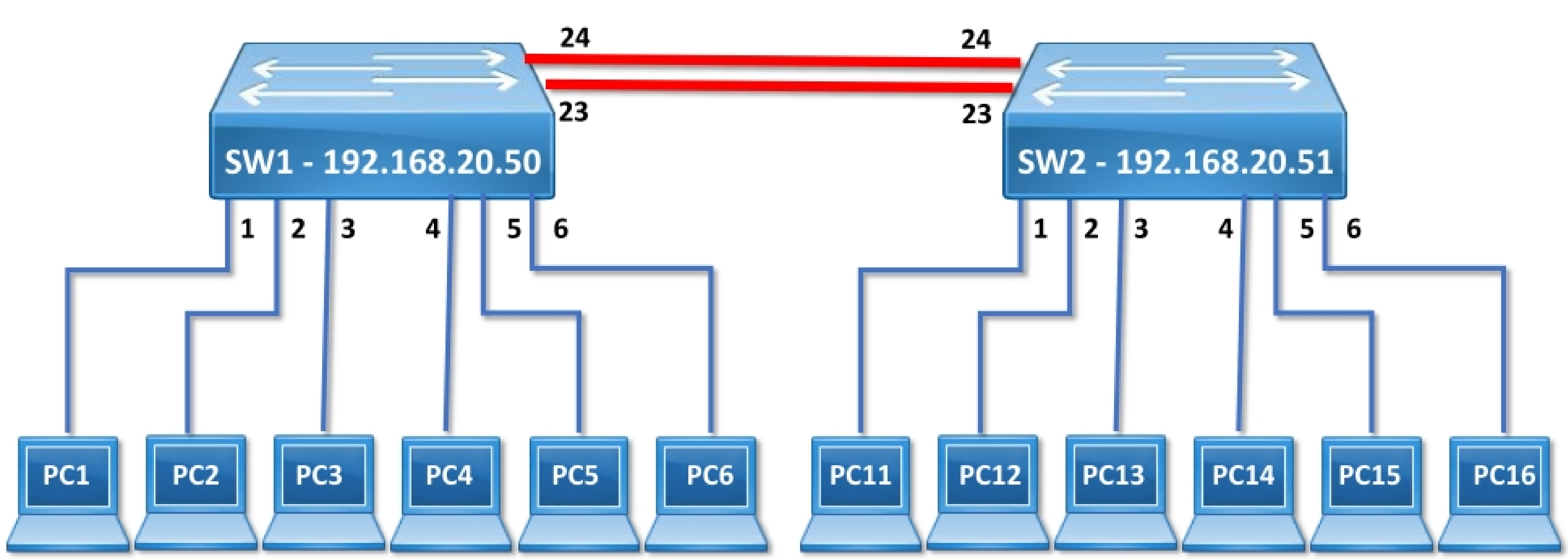
To configure a switch as a Root Switch

Switch (config) # spanning-tree vlan 1 root { primary | secondary }

CCIE CCNP CCNA

STP - Configuration

ZOOM TECHNOLOGIES



CCIE CCNP CCNA

STP - Configuration

ZOOM TECHNOLOGIES

SW1 (config) # spanning-tree vlan 1 root primary

SW1 (config) # spanning-tree vlan 1 root secondary

CCIE CCNP CCNA

STP - Verification

ZOOM TECHNOLOGIES

Switch # show spanning-tree

CCIE CCNP CCNA

Types of Spanning Tree Protocols

- Common Spanning Tree (CST)
  - Open Standard - IEEE 802.1D
  - One spanning-tree instance for entire switch network regardless of the number of vlans.
- Per Vlan Spanning Tree (PVST+)
  - Cisco Proprietary
  - Spanning tree instance for each vlan configured in network
- RSTP
  - Open standard - IEEE 802.1w
  - Enhanced version of STP.
  - Adding roles to ports and enhances to BPDU exchanges.

Types of spanning tree protocols

- Rapid PVST (RPVSTP)
  - A cisco enhancement of RSTP using PVST+
- Mutiple Spanning Tree (MST)
  - Open standard - IEEE 802.1s,
  - Maps multiple VLANs to same spanning tree instance.

Comparison of spanning tree protocols

Protocol	Standard	Resources needed	Convergence	Number of STP Instances
STP	802.1D	Low	Slow	One
PVST+	Cisco	High	Slow	One for every VLAN
RSTP	802.1W	Medium	Fast	One
Rapid PVST+	Cisco	Very high	Fast	One for every VLAN
MST	802.1S	Medium or high	Fast	One for multiple VLAN

Disadvantage of STP – On Access Ports

- Spanning-Tree protocol is running by default on all ports of the switch.
- The spanning-tree protocol makes each port wait up to 50 seconds before data is sent on the port.
- This delay in turn can cause problems with some applications/protocols.
- To solve above issue, Portfast can be implemented on Cisco Switches.

PortFast

- Portfast allows a port to switch from disabled to forwarding state bypassing the listening and learning states.
- The portfast feature can be enabled on a port where there are no Bridges and switches connected, otherwise it may create loops.
- Portfast is recommended to be enabled on a port where end user devices (hosts) are connected.

Portfast - Configuration

Configure Portfast for a Switch (All Interfaces)

Switch (config) # spanning-tree portfast default

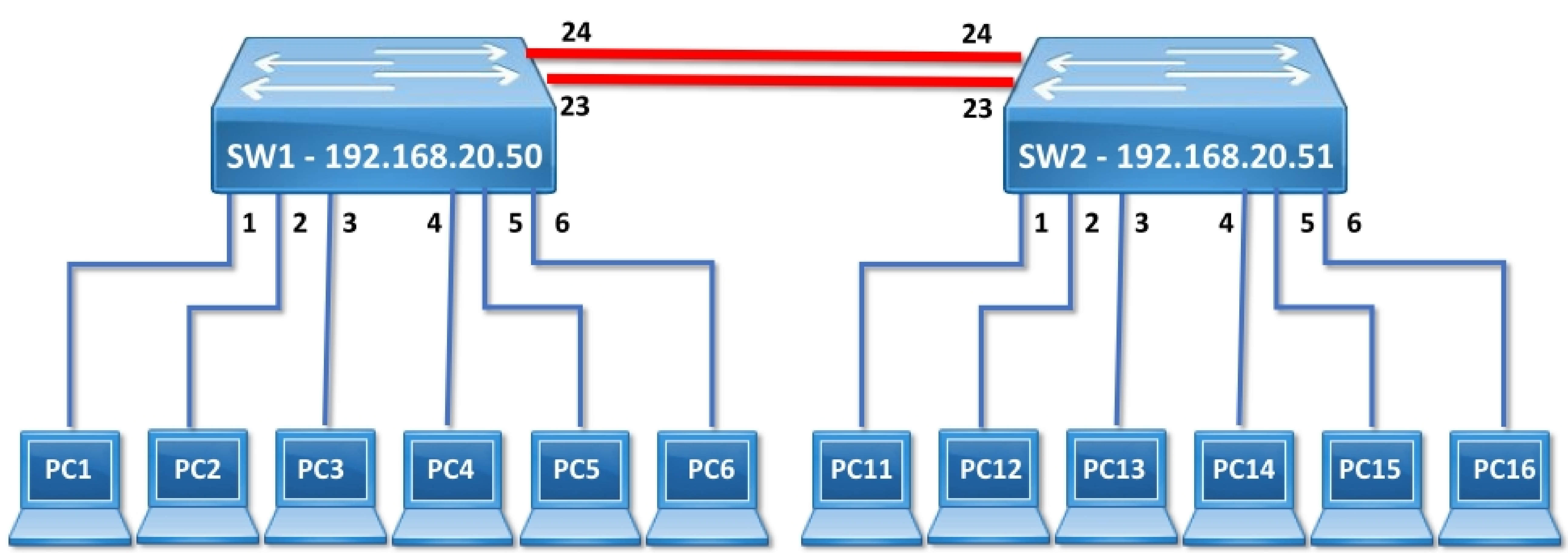
Configure Portfast for an interface

Switch (config) # interface <interface type> <interface no.>

Switch (config-if) # spanning-tree portfast

Switch (config-if) # end

Portfast - Configuration



Portfast - Verification

Switch # show spanning-tree

Switch # show spanning-tree summary

BPDU Guard

- **The Cisco BPDU guard feature disables the port, if any BPDUs are received on the port.**
- **This is recommended to be enabled on a port where Portfast is configured, because if any switch connects to such a port, the local switch can block the port preventing loops.**

BPDU Guard - Configuration

Configure BPDU Guard for a Switch (All Interfaces)

Switch (config) # spanning-tree bpduguard default

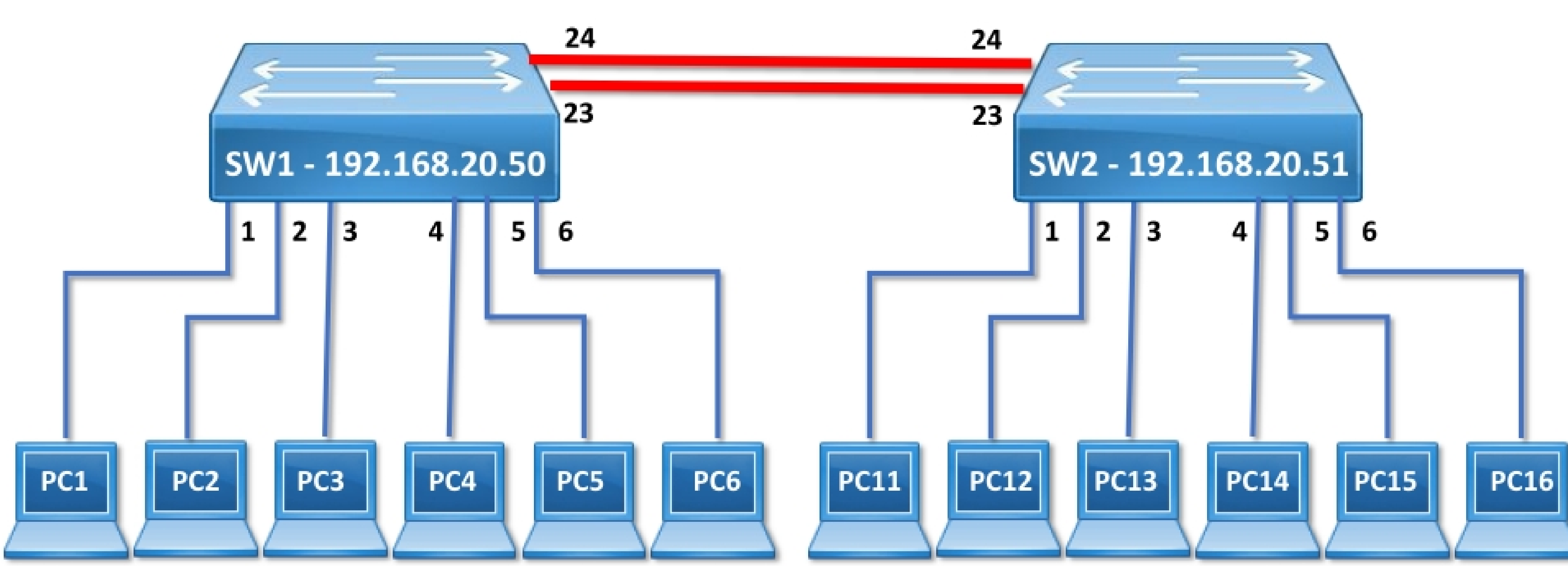
Configure BPDU Guard for an interface

Switch (config) # interface <interface type> <interface no.>

Switch (config-if) # spanning-tree portfast bpduguard enable

Switch (config-if) # end

BPDU Guard - Configuration



BPDU Guard - Verification

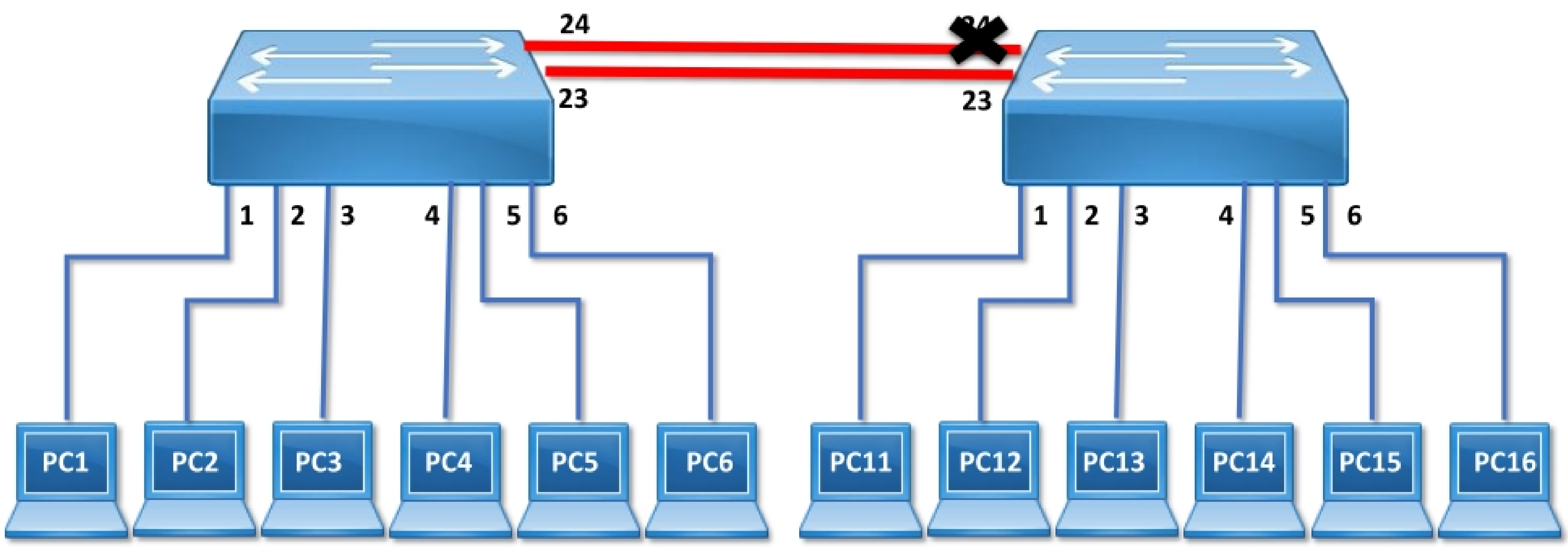
Switch # show spanning-tree

Switch # show spanning-tree summary

Issue with Redundant Link

ZOOM TECHNOLOGIES

- To avoid a single point of failure we go with redundancy. But whenever the redundant link is seen switch blocks a link to avoid loops.



CCIE CCNP CCNA

Etherchannel

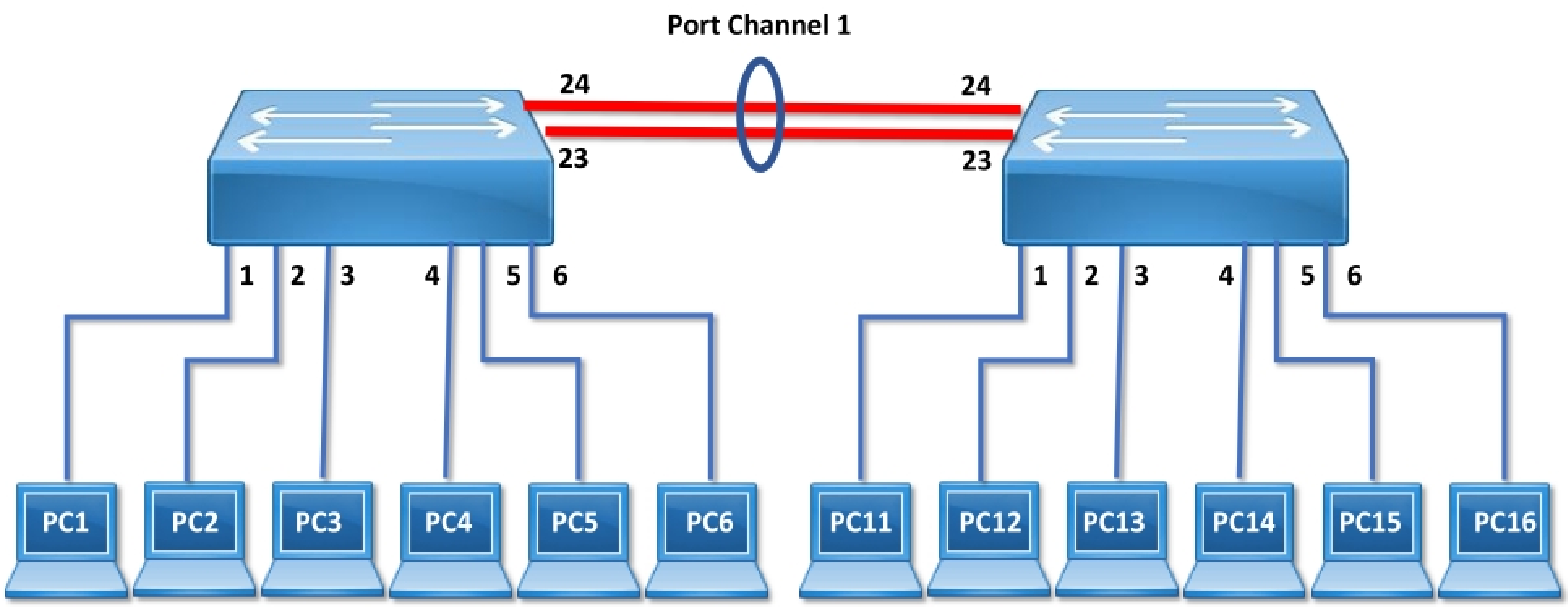
ZOOM TECHNOLOGIES

- Etherchannel combines two or more physical links into one logical link.
- The purposes of aggregating link is achieve the full bandwidth, load balancing and redundancy.
- Generally configured between switch to switch, switch to router, switch to firewall.
- Etherchannels can consist of up to eight interfaces.
- To create etherchannel all the ports needs :
  - Same Physical ports (Ethernet or Fiber)
  - Speed
  - Duplex
  - Either ports should be access or trunk
  - Native and allowed vlan on trunk ports

CCIE CCNP CCNA

Etherchannel

ZOOM TECHNOLOGIES



CCIE CCNP CCNA

Etherchannel Configuration

ZOOM TECHNOLOGIES

- **Static**
- **Port Aggregation Protocol (PAGP)**
- **Link aggregation control protocol (LACP)**

CCIE CCNP CCNA

Port Aggregation Protocol (PAGP)

- It is a cisco proprietary.
- It has two modes
  - Desirable
    - Interface will actively ask the other side to form Etherchannel.
  - Auto
    - Interface will wait passively for other side to ask to form Etherchannel.

PAgP

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

Link Aggregation Control Protocol (LACP)

- It is an open standard protocol (IEEE 802.3ad)
- It has two modes
  - Active
    - Interface will actively ask the other side to form Etherchannel.
  - Passive
    - Interface will wait passively for other side to ask to form Etherchannel.

LACP

	Active	Passive
Active	Yes	Yes
Passive	Yes	No

Etherchannel - Configuration

ZOOM TECHNOLOGIES

Etherchannel – PAGP

Switch (config) # interface <interface type> <interface no.>
Switch (config-if) # channel-protocol pagp
Switch (config-if) # channel-group 1 mode { desirable | auto }
Switch (config-if) # end

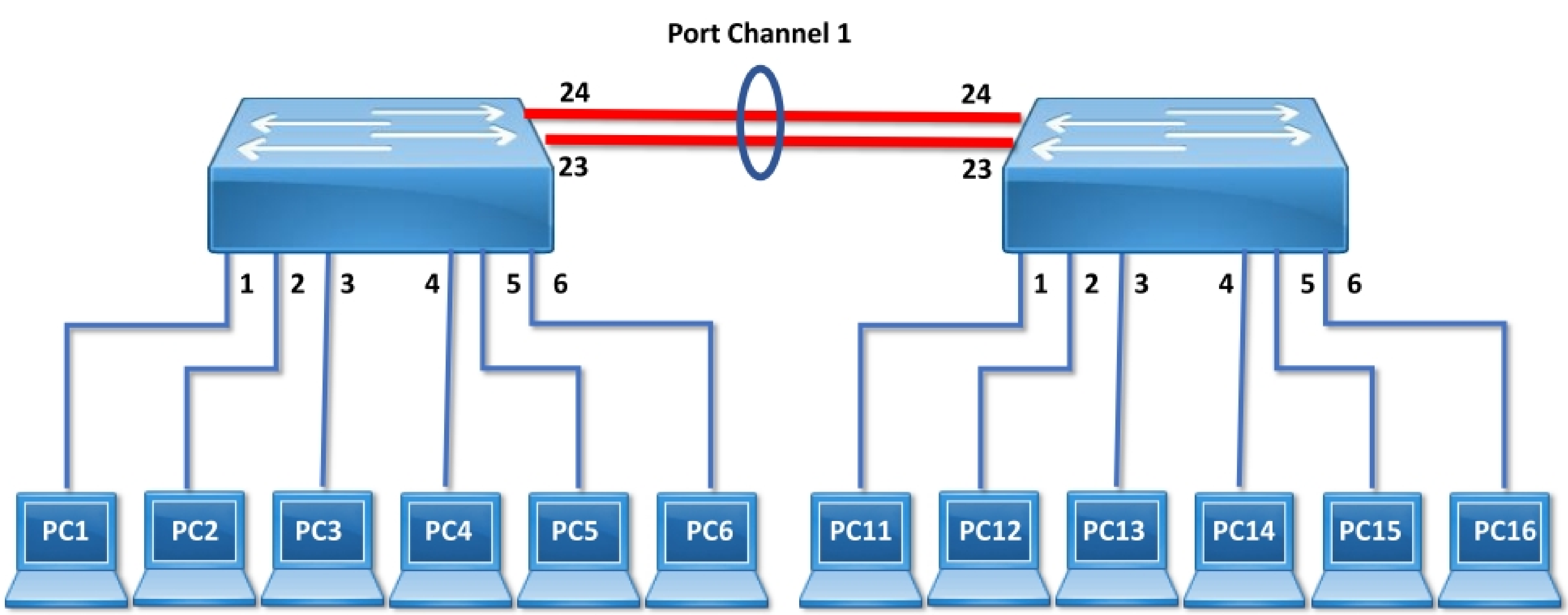
Etherchannel – LACP

Switch (config) # interface <interface type> <interface no.>
Switch (config-if) # channel-protocol lacp
Switch (config-if) # channel-group 1 mode { active | passive }
Switch (config-if) # end

CCIE CCNP CCNA

Etherchannel - Configuration

ZOOM TECHNOLOGIES



CCIE CCNP CCNA

Etherchannel - Configuration

SW1

```
Switch (config) #  interface range fastethernet 0/23
Switch (config-if) #  channel-protocol pagp
Switch (config-if) #  channel-group 1 mode  desirable
Switch (config) #  interface range fastethernet 0/24
Switch (config-if) #  channel-protocol pagp
Switch (config-if) #  channel-group 1 mode  desirable
Switch (config-if) # end
```

SW2

```
Switch (config) #  interface range fastethernet 0/23
Switch (config-if) #  channel-protocol pagp
Switch (config-if) #  channel-group 1 mode  auto
Switch (config) #  interface range fastethernet 0/24
Switch (config-if) #  channel-protocol auto
Switch (config-if) #  channel-group 1 mode  desirable
Switch (config-if) # end
```

SW1

```
Switch (config) #  interface range fastethernet 0/23
Switch (config-if) #  channel-protocol lacp
Switch (config-if) #  channel-group 1 mode  active
Switch (config) #  interface range fastethernet 0/24
Switch (config-if) #  channel-protocol lacp
Switch (config-if) #  channel-group 1 mode  active
Switch (config-if) # end
```

SW2

```
Switch (config) #  interface range fastethernet 0/23
Switch (config-if) #  channel-protocol lacp
Switch (config-if) #  channel-group 1 mode  passive
Switch (config) #  interface range fastethernet 0/24
Switch (config-if) #  channel-protocol lacp
Switch (config-if) #  channel-group 1 mode  passive
Switch (config-if) # end
```

Etherchannel - Verification

```
Switch #  show etherchannel 1 summary
Switch #  show interface port-channel 1
Switch #  show etherchannel port-channel
```

Port Security

- **Port Security is used to control network access based on the following:**
  - **MAC Address**
  - **Number of MAC Addresses per port**
- **If any violation takes place the following actions can be configured:**
  - **Shutdown**
  - **Restrict**
  - **Protect**

Violation Modes

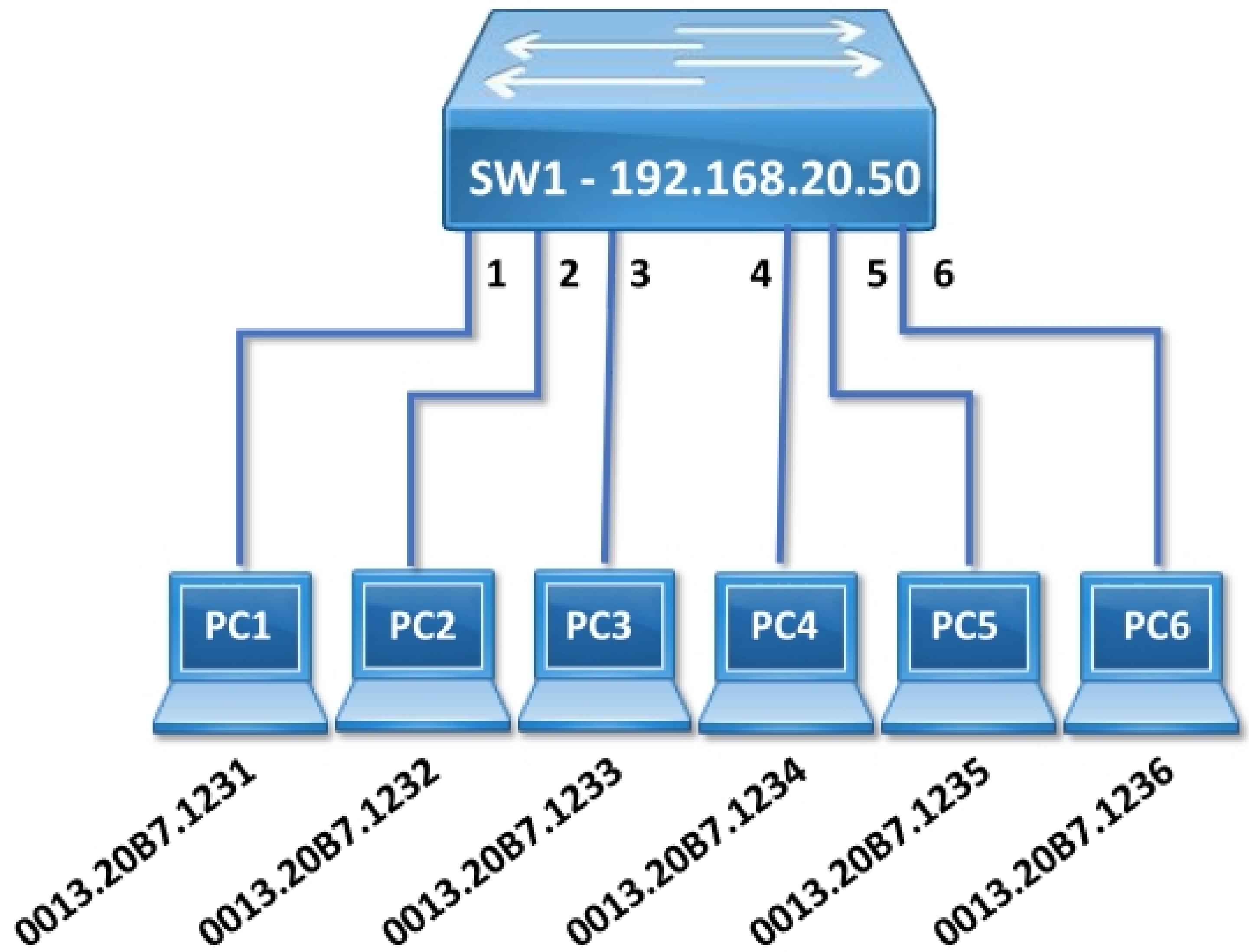
- **Shutdown**
  - The port becomes error disabled and the port LED turns off.
- **Protect**
  - Frames with unknown source MAC address are dropped. It does not notify that a security violation has occurred.
- **Restrict**
  - Frames with unknown source address are dropped. It gives a notification (log message) that security violation has occurred.

Port Security & Error Recovery - Configuration

```
Switch (config) #  interface  <interface type>  <interface no.>
Switch (config-if) #  switchport  mode access
Switch (config-if) #  switchport port-security maximum <value>
Switch (config-if) #  switchport port-security mac-address <mac-address>
Switch (config-if) #  switchport port-security violation { protect | restrict |
                      shutdown }
Switch (config-if) #  switchport  port-security
```

```
Switch (config) #  errdisable recovery cause <cause>
Switch (config) #  errdisable recovery interval <seconds>
```

Port Security & Error Recovery - Configuration



Port Security & Error Recovery - Configuration


```
SW1 (config)# interface fastethernet 0/2
SW1 (config-if)# switchport mode access
SW1 (config-if)# switchport port-security maximum 1
SW1 (config-if)# switchport port-security mac-address 0013.20B7.1232
SW1 (config-if)# switchport port-security violation shutdown
SW1 (config-if)# switchport port-security
SW1 (config-if)# exit
SW1 (config) # errdisable recovery cause psecure-violation
SW1 (config) # errdisable recovery interval 30
```

Port Security & Error Recovery - Verification

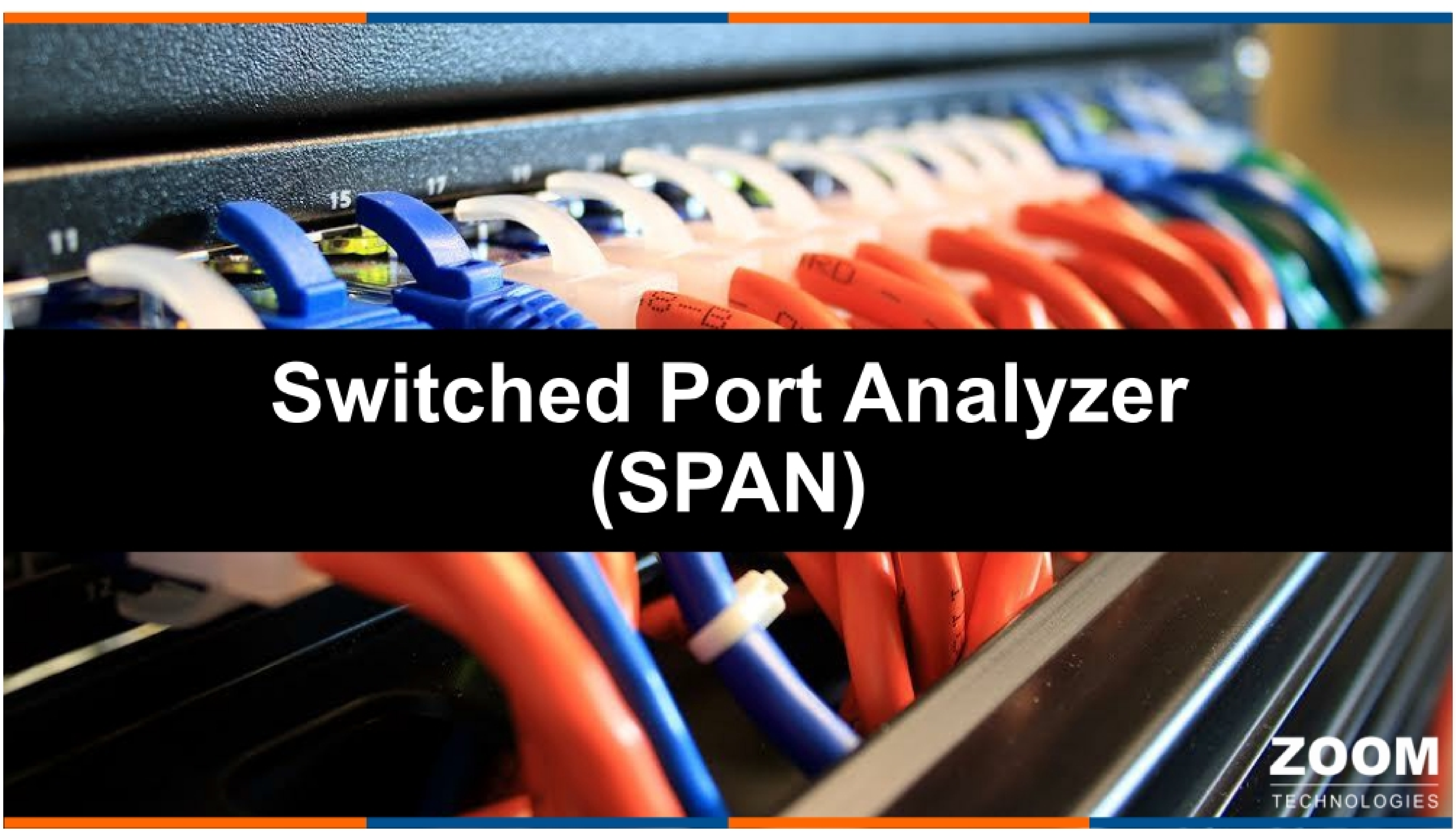
Switch # show port-security interface <interface type> <interface no.>

Switch # show interface status

Switch # show port-security

Switch # show port-security address

Switch # show errdisable recovery



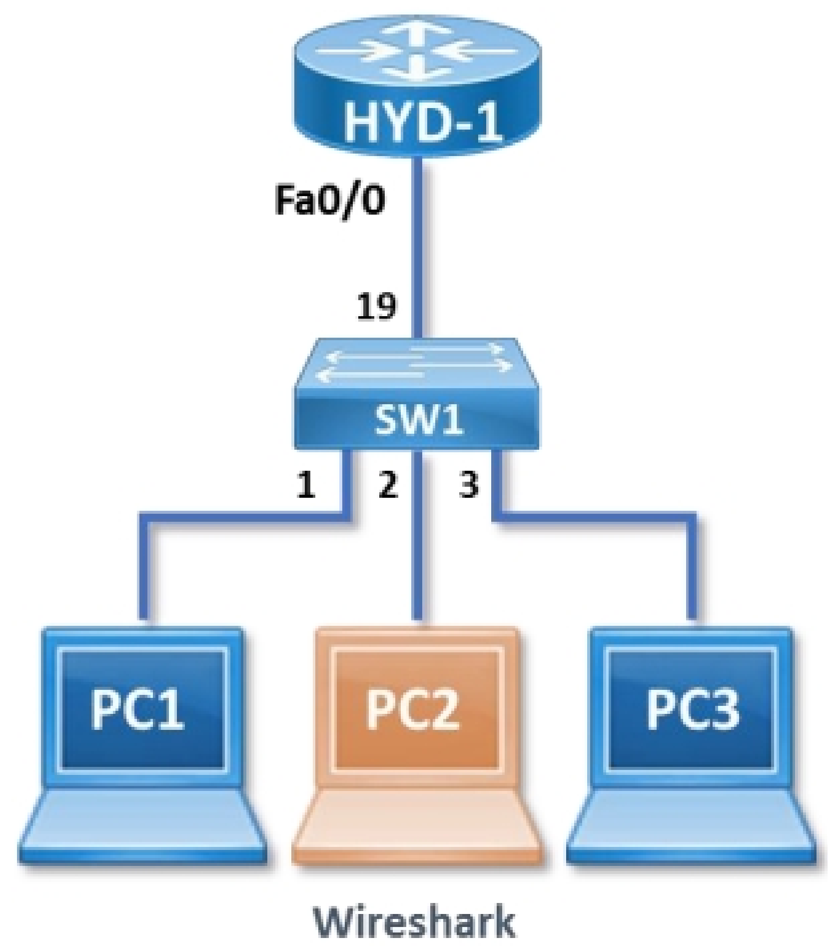
Switched Port Analyzer (SPAN)

- A SPAN port mirrors traffic from a defined port to another port where a Network Anazlyer / Monitoring Device is connected.
- Network engineers or administrators use SPAN to analyze and debug data or diagnose errors on a network.
- Network analyzer software is used for analyzing the captured data. i.e. Wireshark, Ethereal, etc.

SPAN - Configuration

```
Switch (config) #  monitor session <no.> source interface
                   <interface type>  <interface no.>
Switch (config) #  monitor session <no.> destination interface
                   <interface type>  <interface no.>
```

SPAN - Configuration



SPAN - Configuration

SW1

SW1 (config) # monitor session 1 source interface FastEthernet 0/11

SW1 (config) # monitor session 1 destination interface FastEthernet 0/2

SPAN - Verification

Switch (config) # show monitor

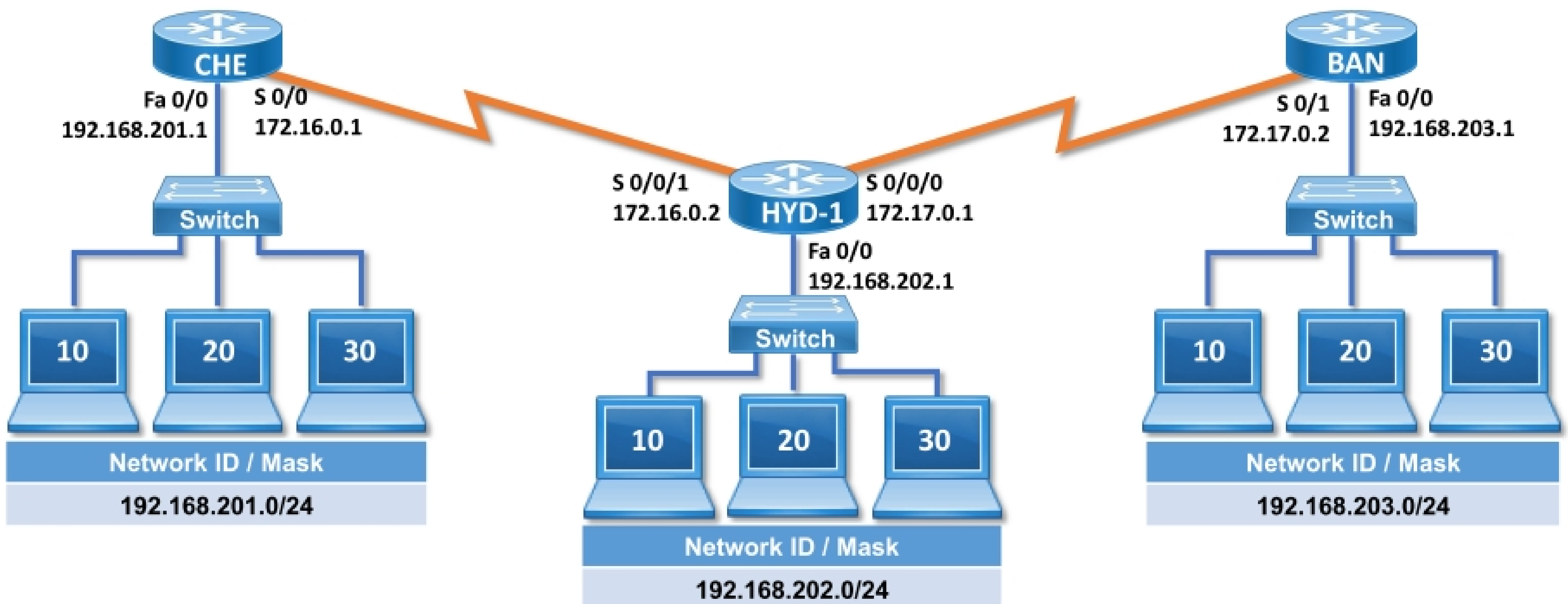
Access Control List (ACL)

- Access Control List are a group of commands configured on router to control the flow of traffic from one network to another network.
- It provides layer 3 and layer 4 security.
- The router examines each packet to determine whether to forward or drop it, based on the conditions specified in the ACL.

Functions of ACL's ?

- Controls network traffic to improve network performance
- Provide a basic level of security for network access.
- Can filter traffic based on type of traffic.
  - i.e. ACL can allow Web Traffic and block all Email traffic

Access Control List (ACL)



192.168.203.10 host should not communicate with 192.168.202.0 network

Terminology

- **Deny : Blocking a network/subnet/host/service.**
- **Permit : Allowing a network/subnet/host/service.**
- **Source Address : The address from where the request starts.**
- **Destination address : The address where the request ends.**
- **Inbound : Traffic coming into the interface.**
- **Outbound : Traffic going out of the interface.**

Terminology

- Protocols : IP (Internet Protocol)
  - TCP (Transmission control protocol)
  - UDP (User datagram protocol)
  - ICMP (Internet control messaging protocol)
- Operators :
  - eq (equal to)
  - neq (not equal to)
  - lt (less than)
  - gt (greater than)
- Services : HTTP (80), FTP (20,21), TELNET (23), DNS (53), DHCP (67,68)

Wildcard Mask

- It's the inverse of the subnet mask, hence is also called as inverse mask.
- A bit value of 0 indicates MUST MATCH (Check Bits).
- A bit value of 1 indicates IGNORE (Ignore Bits).
- Wildcard Mask
  - For a host is 0.0.0.0
  - For Class A network is 0.255.255.255
  - For Class B network is 0.0.255.255
  - For Class C network is 0.0.0.255

Wild Card Mask

- A wild card mask can be calculated using the formula :

```
        Global Subnet Mask
   –    Subnet Mask
        ---------------------------
        Wild Card Mask
```

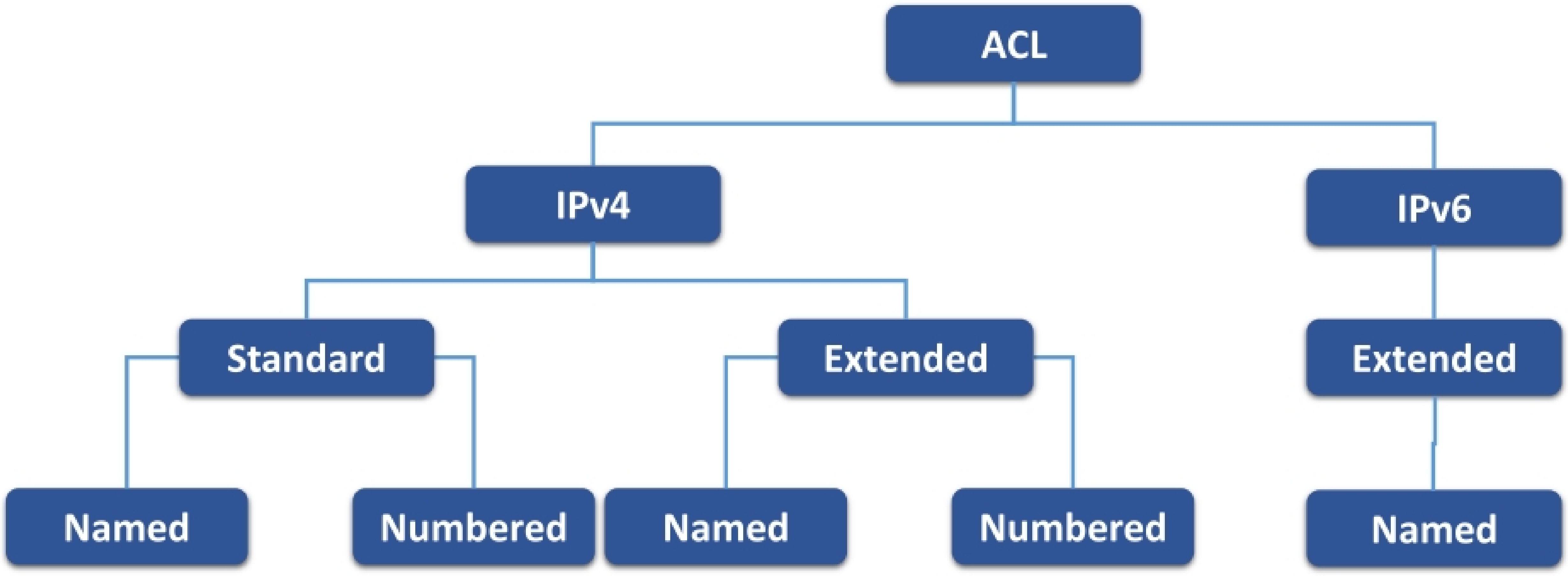
E.g.

```
        255.255.255.255            255.255.255.255
   –    255.255.255.   0         – 255.255.255.240
        ------------------------   ------------------------
         0.    0.    0.255          0.    0.    0.   15
```

Working of Access Control List

- Works in a sequential order from top to bottom.
- If a match is found it does not check further.
- There should be at least one permit statement.
- An implicit deny blocks all traffic by default when there is no match (an invisible statement).
- New entries are automatically added to the bottom.
- Can have one access-list per interface per direction.
- Removing of specific statement in a numbered access-lists is not possible.

Types of Access-List



Standard Access List

- The access-list number range is 1 – 99.
- Can filter a network, subnet or host.
- Two way communication is stopped.
- All services are either blocked or allowed.
- Filters traffic based only on the source address.
- Implemented closest to the destination. (Guideline)

Standard ACL - Numbered - Configuration

Creation of Standard Access List - Numbered

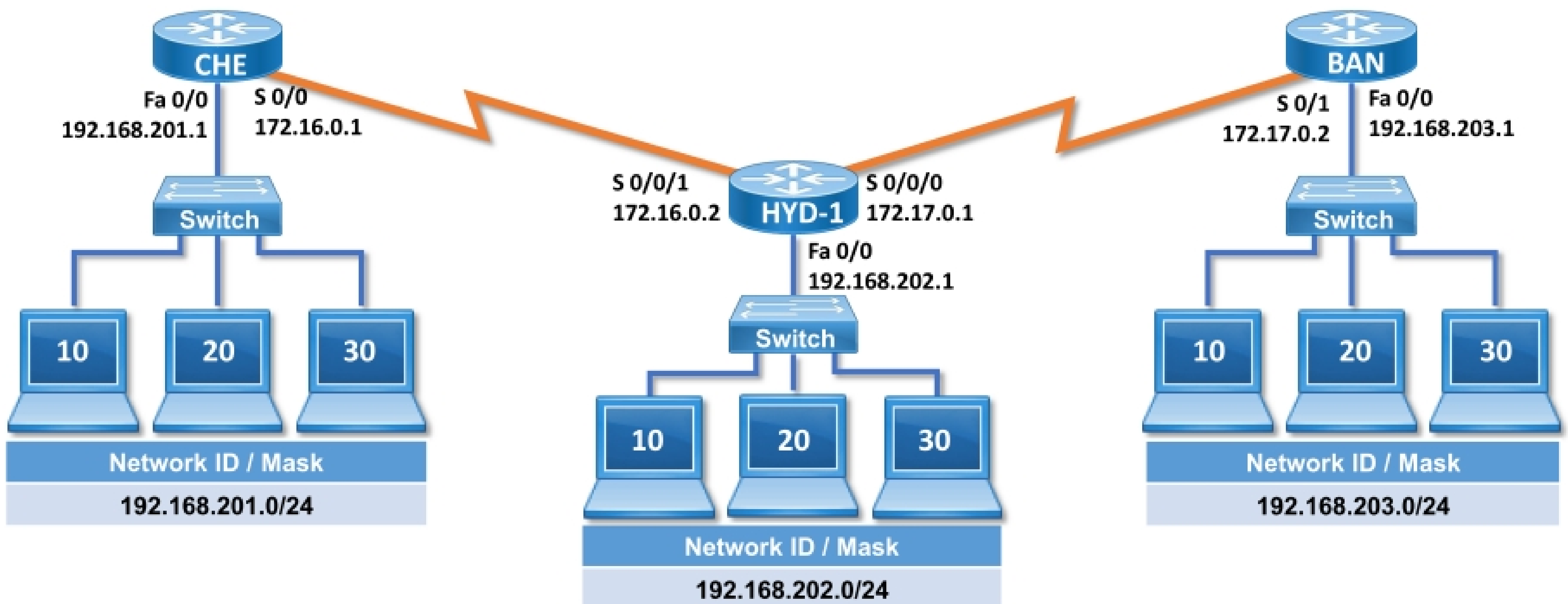
Router (config) # access-list <acl no> <permit/deny>
<source address> <source wildcard mask>

Implementation of Standard Access List - Numbered

Router (config) # interface <interface type> <interface no>
Router(config-if) # ip access-group <number> <out/in>

Standard ACL - Numbered - Configuration

ZOOM TECHNOLOGIES



192.168.201.10 host should not communicate with 192.168.202.0 network

CCIE CCNP CCNA

Standard ACL - Numbered - Configuration

ZOOM TECHNOLOGIES

HYD-1

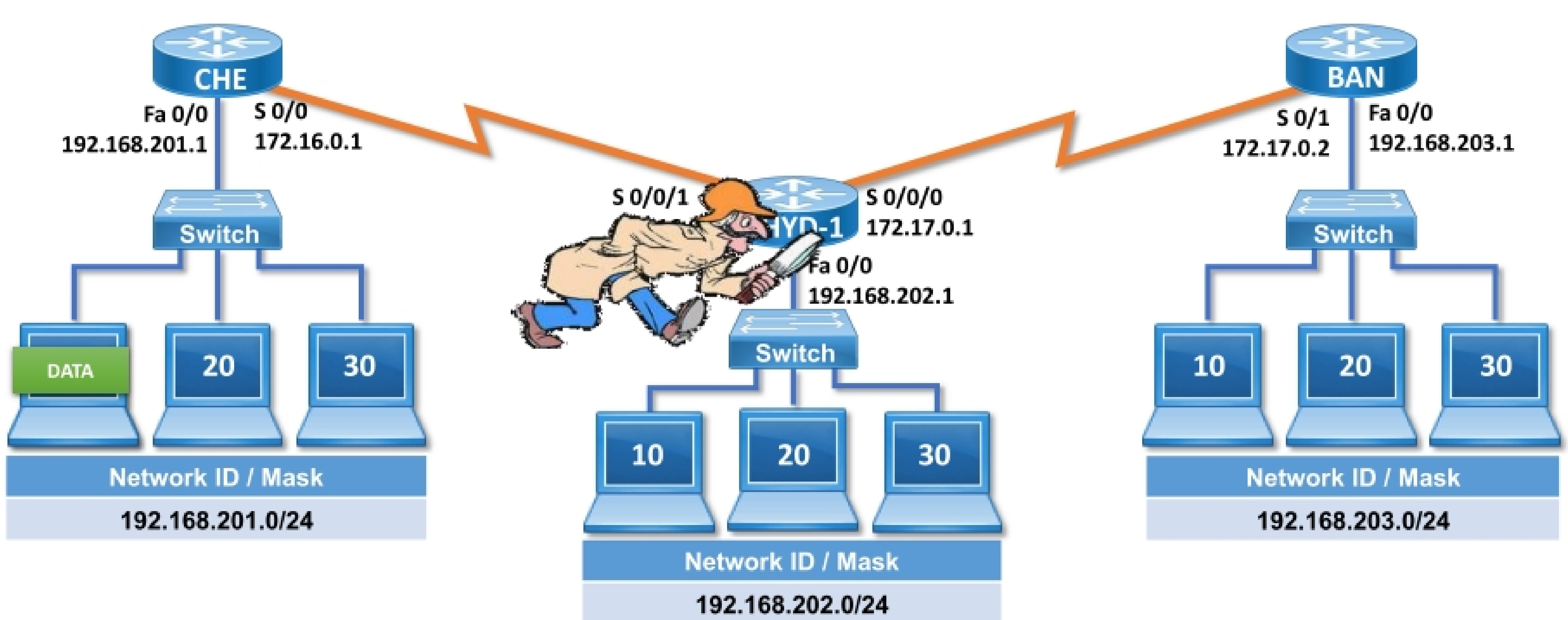
```
HYD-1 # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HYD-1 (config) # access-list 10 deny 192.168.201.10 0.0.0.0
HYD-1 (config) # access-list 10 permit any
HYD-1 (config) #

HYD-1 (config) # interface FastEthernet 0/0
HYD-1 (config-if) # ip access-group 1 out
HYD-1 (config-if) # end
HYD-1 #
```

CCIE CCNP CCNA

Standard ACL - Numbered - Verification

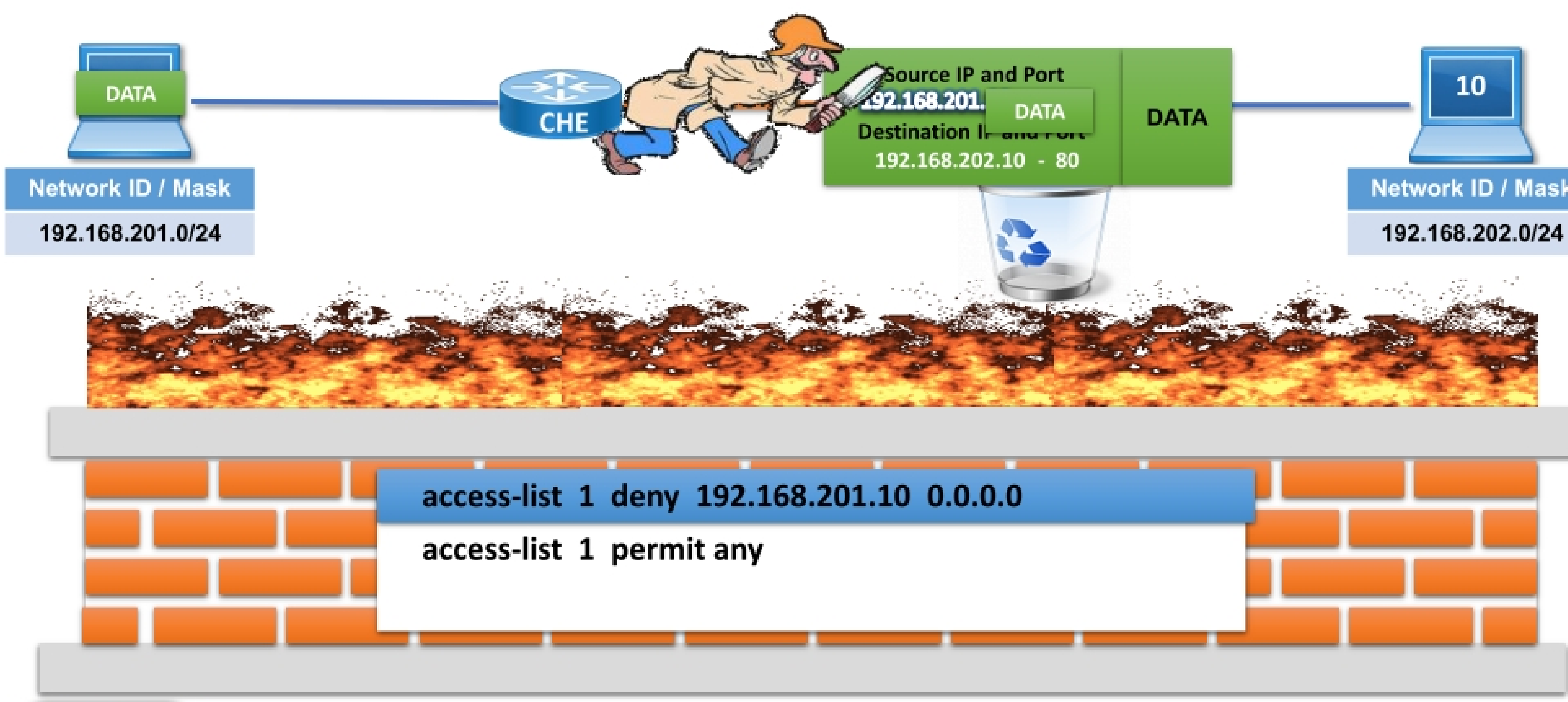
Router # show ip access-lists

How does a Standard ACL work ?

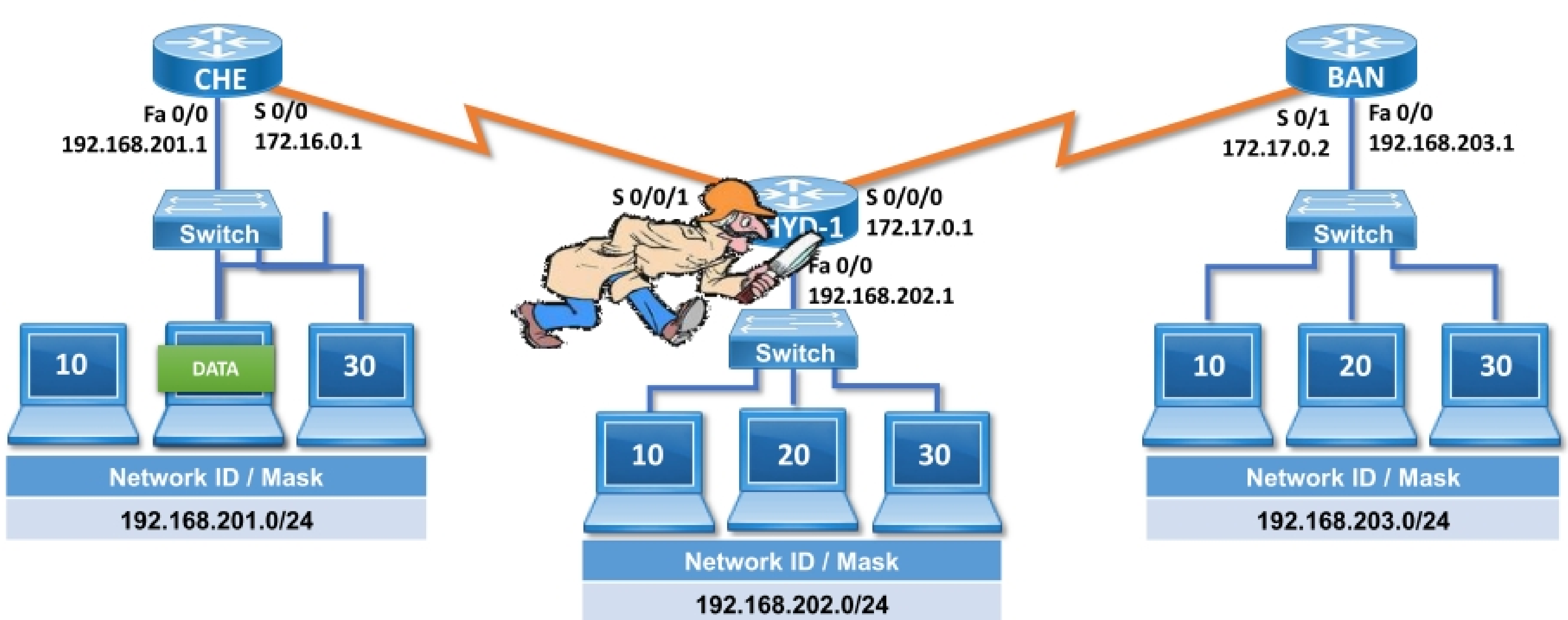


192.168.201.10 is accessing 192.168.202.20

How does a Standard ACL work ?

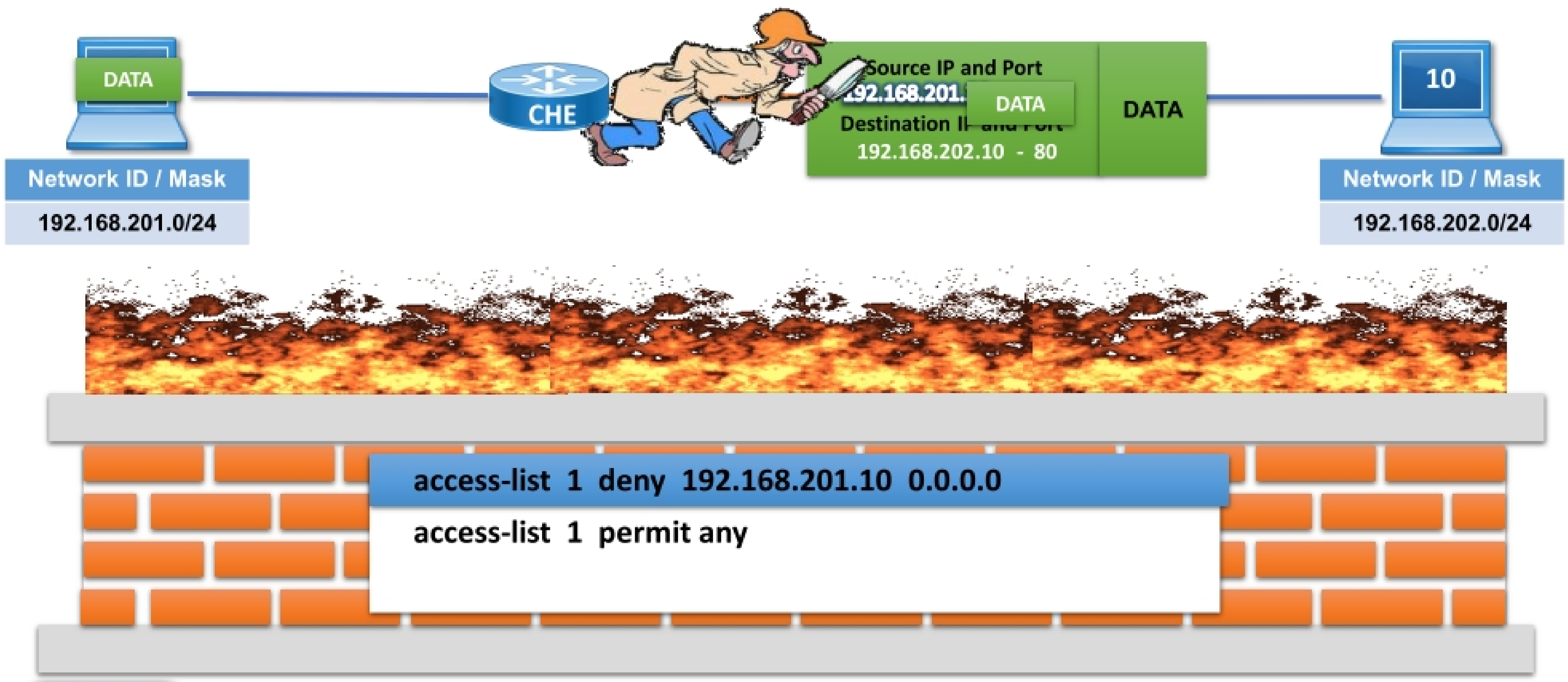


How does a Standard ACL work ?



192.168.201.20 is accessing 192.168.202.20

How does a Standard ACL work ?



Standard ACL - Named- Configuration

Creation of Standard Access List - Named

Router (config) # ip access-list standard <acl name>

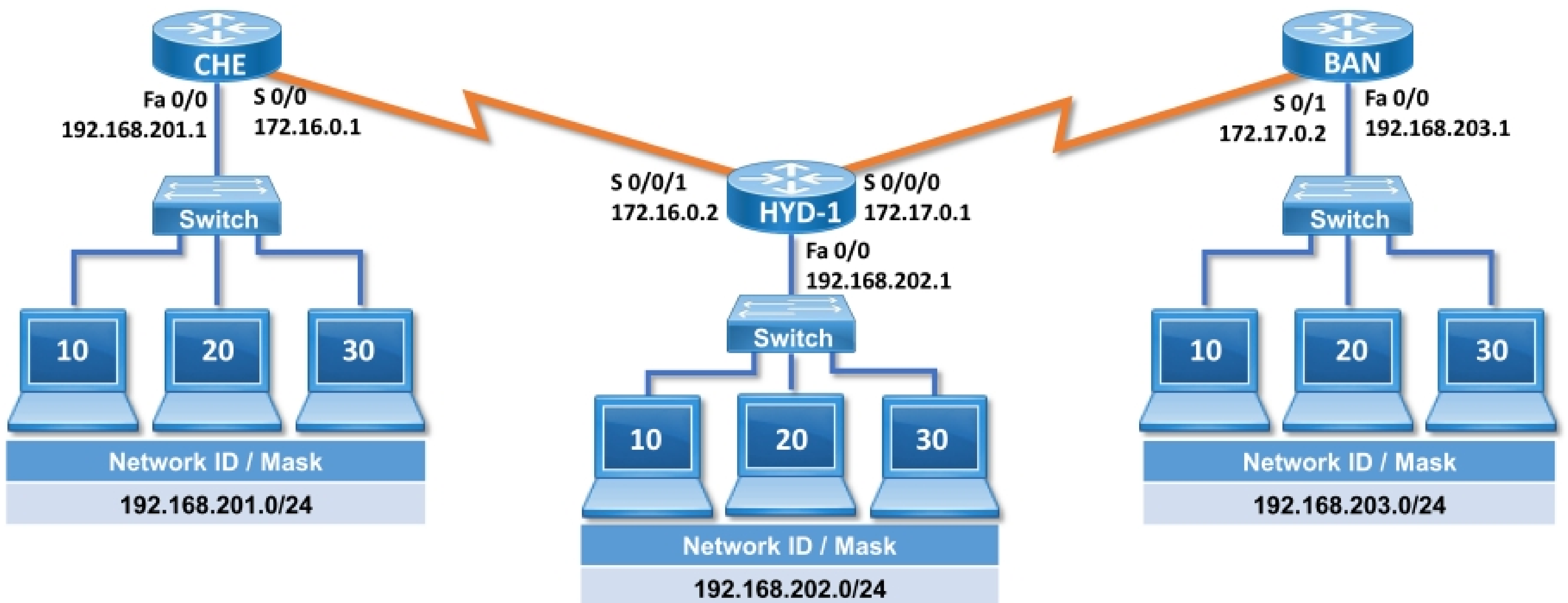
Router (config-std-nacl) # <permit/deny> <source address> <source wildcard mask>

Implementation of Standard Access List - Named

Router (config) # interface <interface type> <interface no>

Router(config-if) # ip access-group <acl name> <out/in>

Standard ACL - Named- Configuration



192.168.203.10 host should communicate with 192.168.202.0 network

Standard ACL - Named- Configuration

HYD-1

```
HYD-1 # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HYD-1 (config) # ip access-list standard zoom
HYD-1 (config-std-nacl) # permit 192.168.203.10 0.0.0.0
HYD-1 (config-std-nacl) # exit
HYD-1 (config) #

HYD-1 (config) # interface fastethernet 0/0
HYD-1 (config-if) # ip access-group zoom out
HYD-1 (config-if) # end
HYD-1 #
```

Standard ACL - Named - Verification

Router # show ip access-lists

Extended Access List

- The access-list number range is 100 – 199.
- Can filter a network, subnet, host and service.
- One way communication is stopped.
- Selected services can be blocked or allowed.
- Filters traffic based on the source address, destination address and service.
- Implemented closest to the source. (Guideline)

Extended ACL - Numbered - Configuration

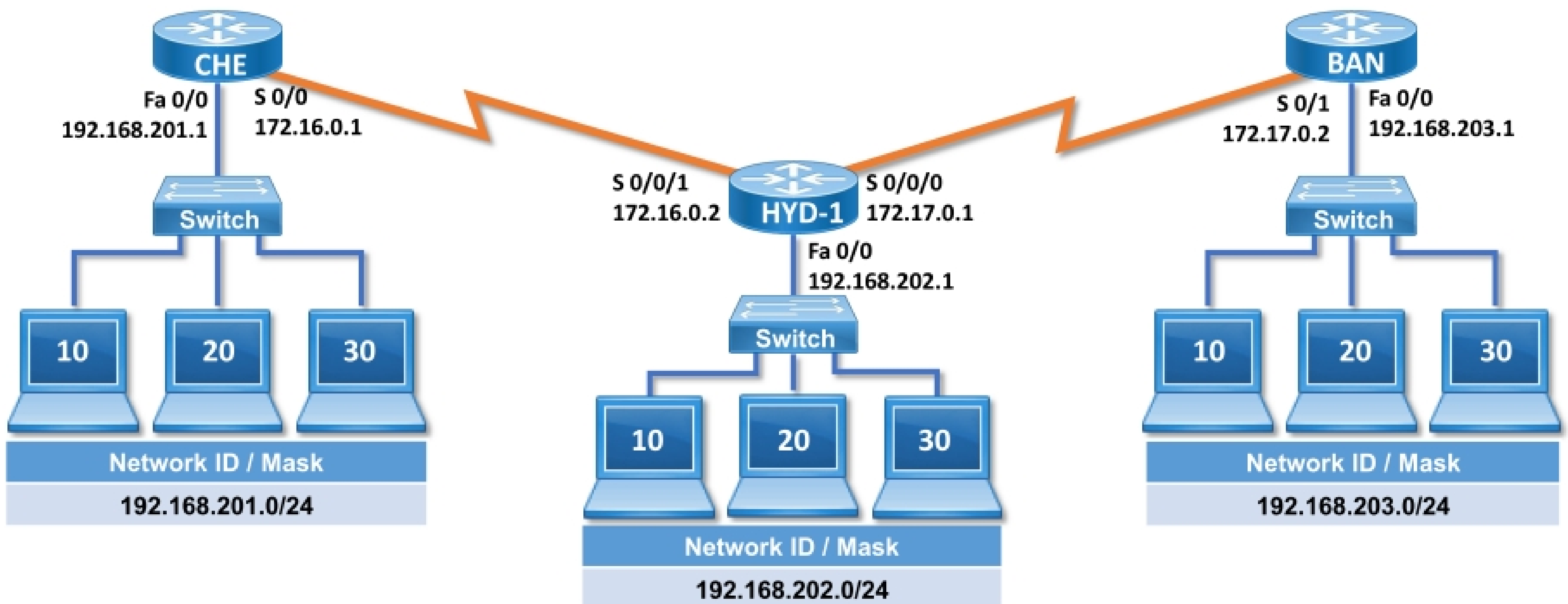
Creation of Extended Access List - Numbered

Router (config) # access-list <acl no> <permit/deny> <protocol>
<source address> <source wildcard mask>
<destination address> < destination wildcard mask>
<operator> <service>

Implementation of Extended Access List - Numbered

Router (config) # interface <interface type> <interface no>
Router(config-if) # ip access-group <number> <out/in>

Extended ACL - Numbered - Configuration



192.168.202.0 network should not access 192.168.203.10 Host (Web service)

192.168.202.0 network should not ping 192.168.201.0 Network

Extended ACL - Numbered - Configuration

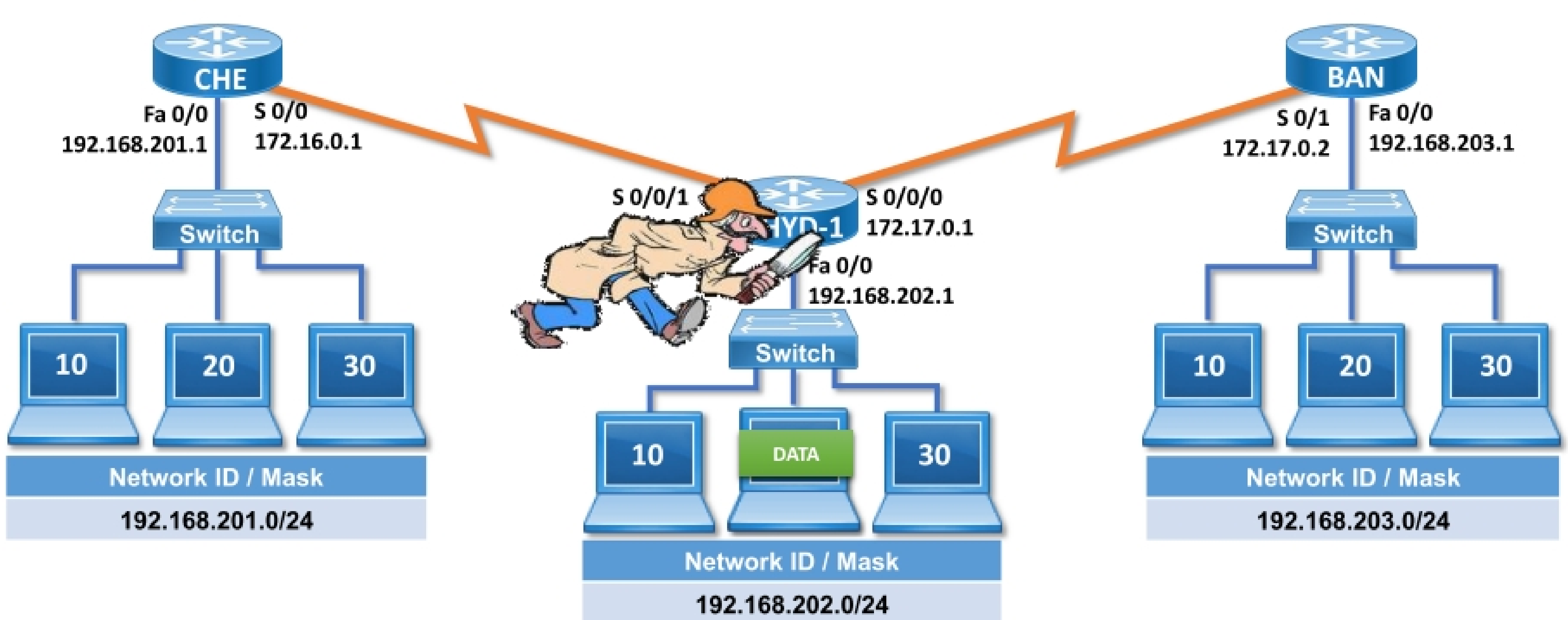
HYD-1

```
HYD-1 # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HYD-1 (config) # access-list 101 deny tcp 192.168.202.0 0.0.0.255 192.168.203.10 0.0.0.0 eq www
HYD-1 (config) # access-list 101 deny icmp 192.168.202.0 0.0.0.255 192.168.201.0 0.0.0.255 echo
HYD-1 (config) # access-list 101 permit ip any any

HYD-1 (config) # interface FastEthernet 0/0
HYD-1 (config-if) # ip access-group 101 in
HYD-1 (config-if) # exit
```

Extended ACL - Numbered - Verification

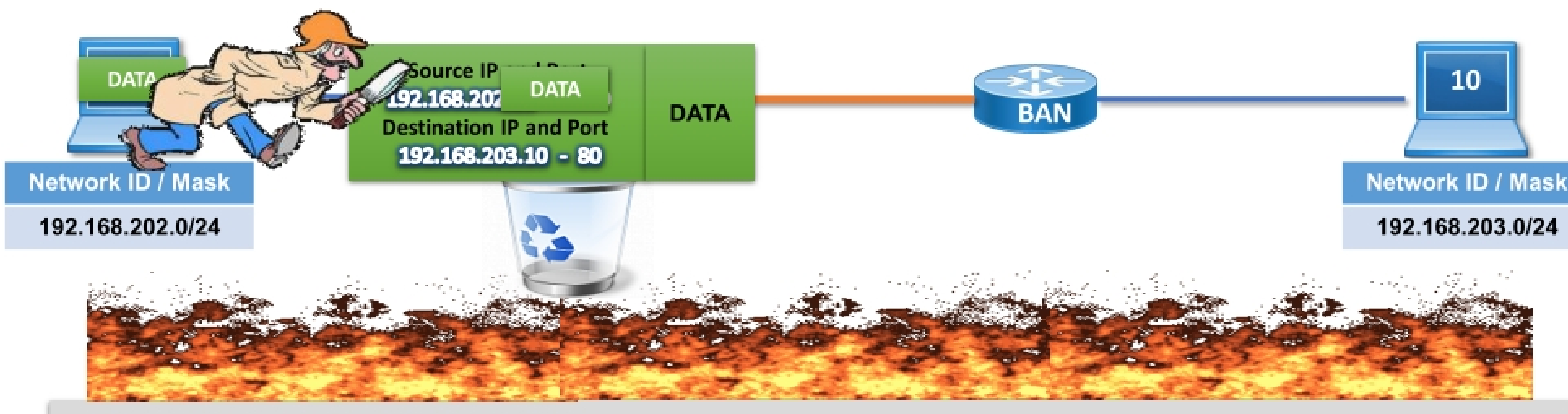
Router # show ip access-lists

How does an Extended ACL work ?



192.168.202.20 is accessing 192.168.203.10 – Web Service

How does an Extended ACL work ?

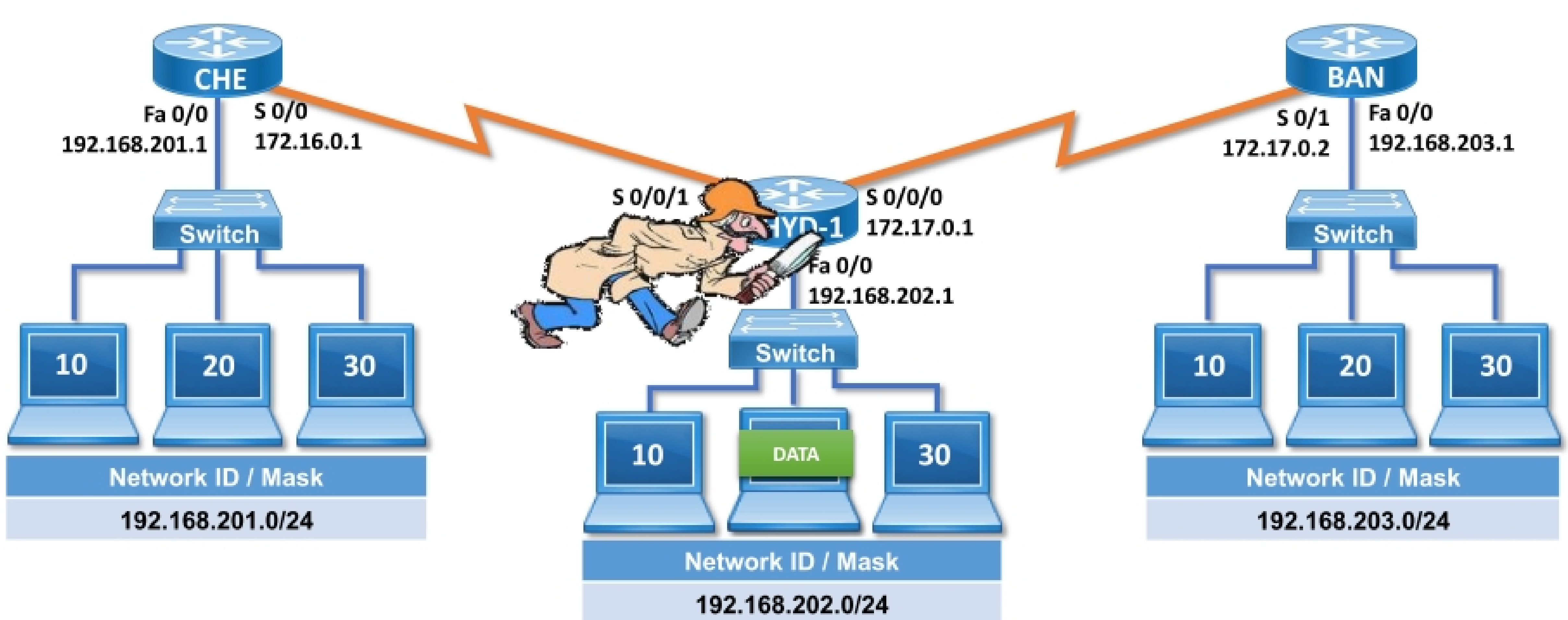


access-list 101 deny tcp 192.168.202.0 0.0.0.255 192.168.203.10 0.0.0.0 eq 80

access-list 101 deny icmp 192.168.202.0 0.0.0.255 192.168.201.0 0.0.0.255 echo

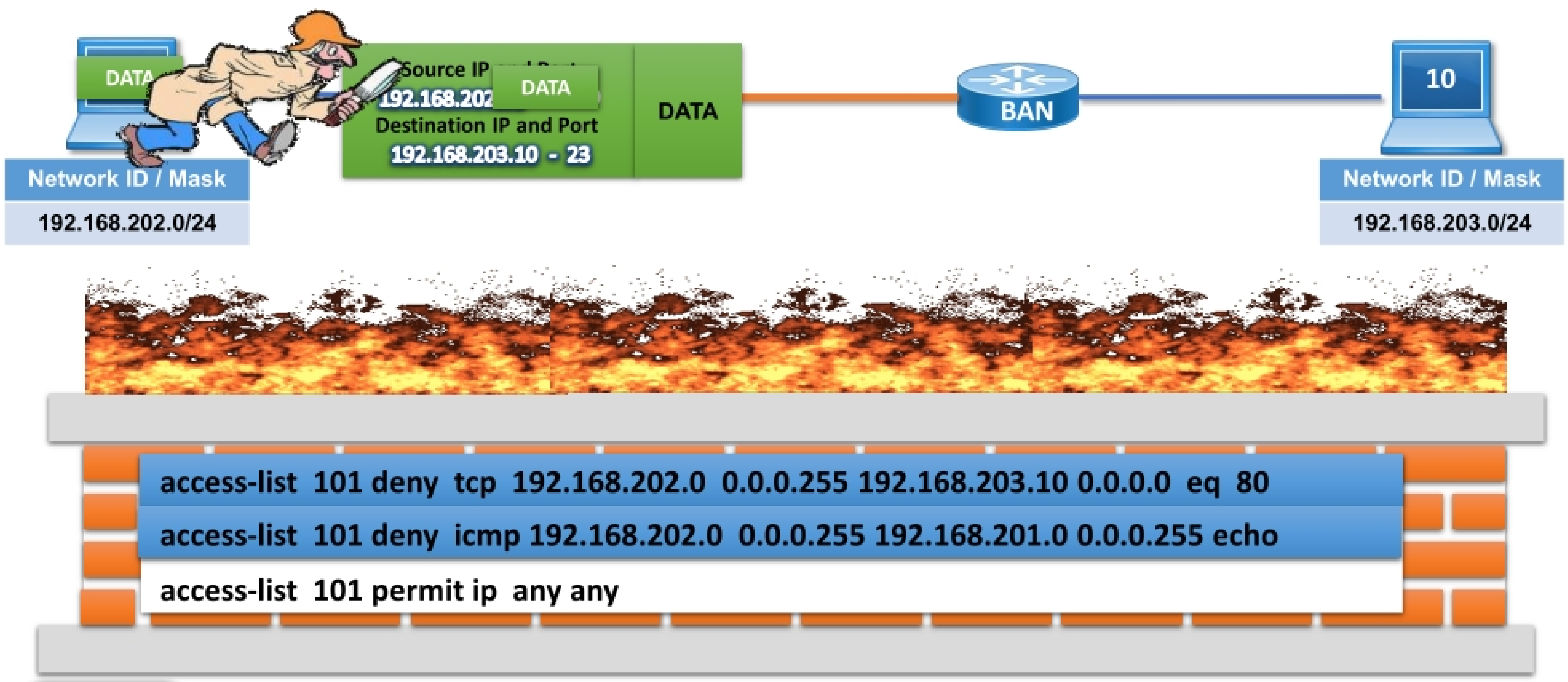
access-list 101 permit ip any any

How does an Extended ACL work ?



192.168.202.20 is accessing 192.168.203.10 – Telnet Service

How does an Extended ACL work ?



Extended ACL - Named - Configuration

Creation of Extended Access List - Named

Router (config) # ip access-list extended <acl name>

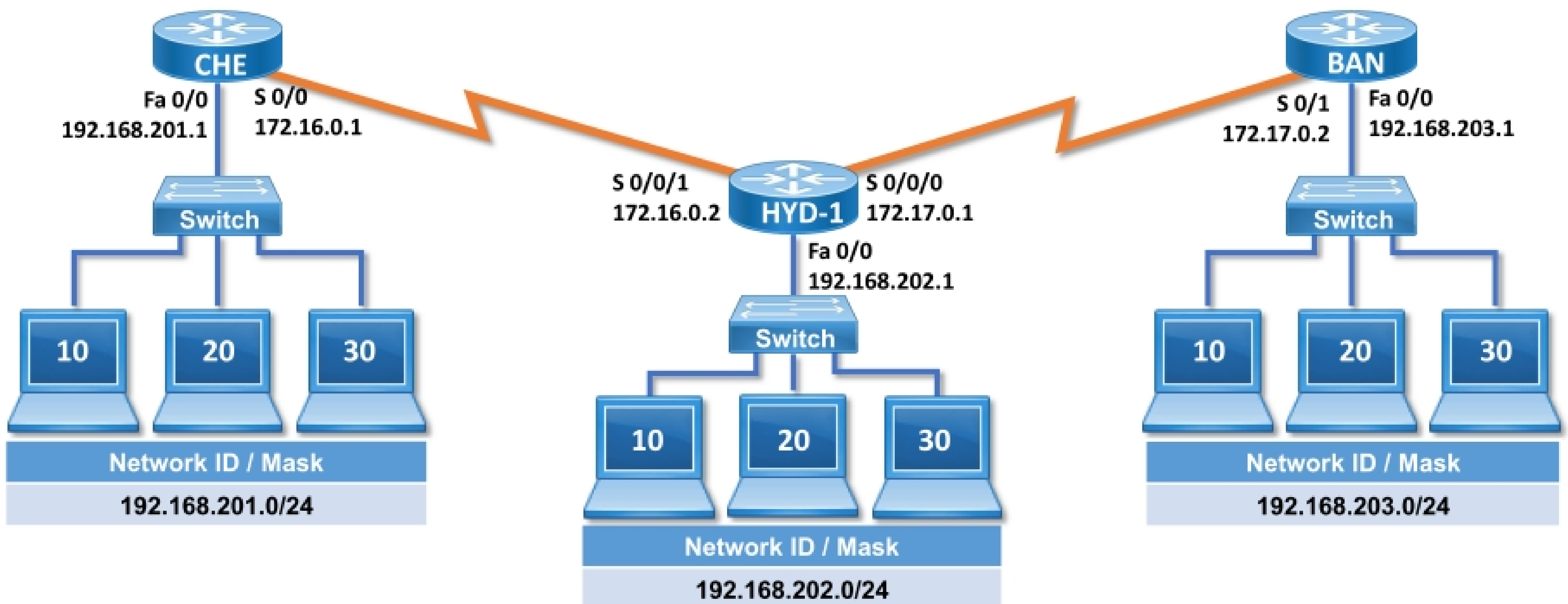
Router (config-ext-nacl) # <permit/deny> <protocol>
<source address> <source wildcard mask>
<destination address> < destination wildcard mask>
<operator> <service>

Implementation of Extended Access List - Named

Router (config) # interface <interface type> <interface no>

Router (config-if) # ip access-group <acl name> <out/in>

Extended ACL - Named - Configuration



Only 192.168.202.10 Host should access 192.168.201.10 Host (FTP service)

192.168.202.0 Network should access any Network (Telnet Service)

Extended ACL - Named - Configuration

HYD-1

```
HYD-1 # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HYD-1 (config) # ip access-list extended cisco
HYD-1(config-ext-nacl) # permit tcp 192.168.202.10 0.0.0.0 192.168.201.10 0.0.0.0 eq ftp
HYD-1(config-ext-nacl) # permit tcp 192.168.202.0 0.0.0.255 any eq telnet
HYD-1(config-ext-nacl) # exit
HYD-1 (config) #

HYD-1 (config) # interface FastEthernet 0/0
HYD-1 (config-if) # ip access-group cisco in
HYD-1 (config-if) # exit
```

Extended ACL - Named - Verification

Router # show ip access-lists

IPv6 ACL - Configuration

Creation of IPv6 Access List

Router (config) # ipv6 access-list <acl name>

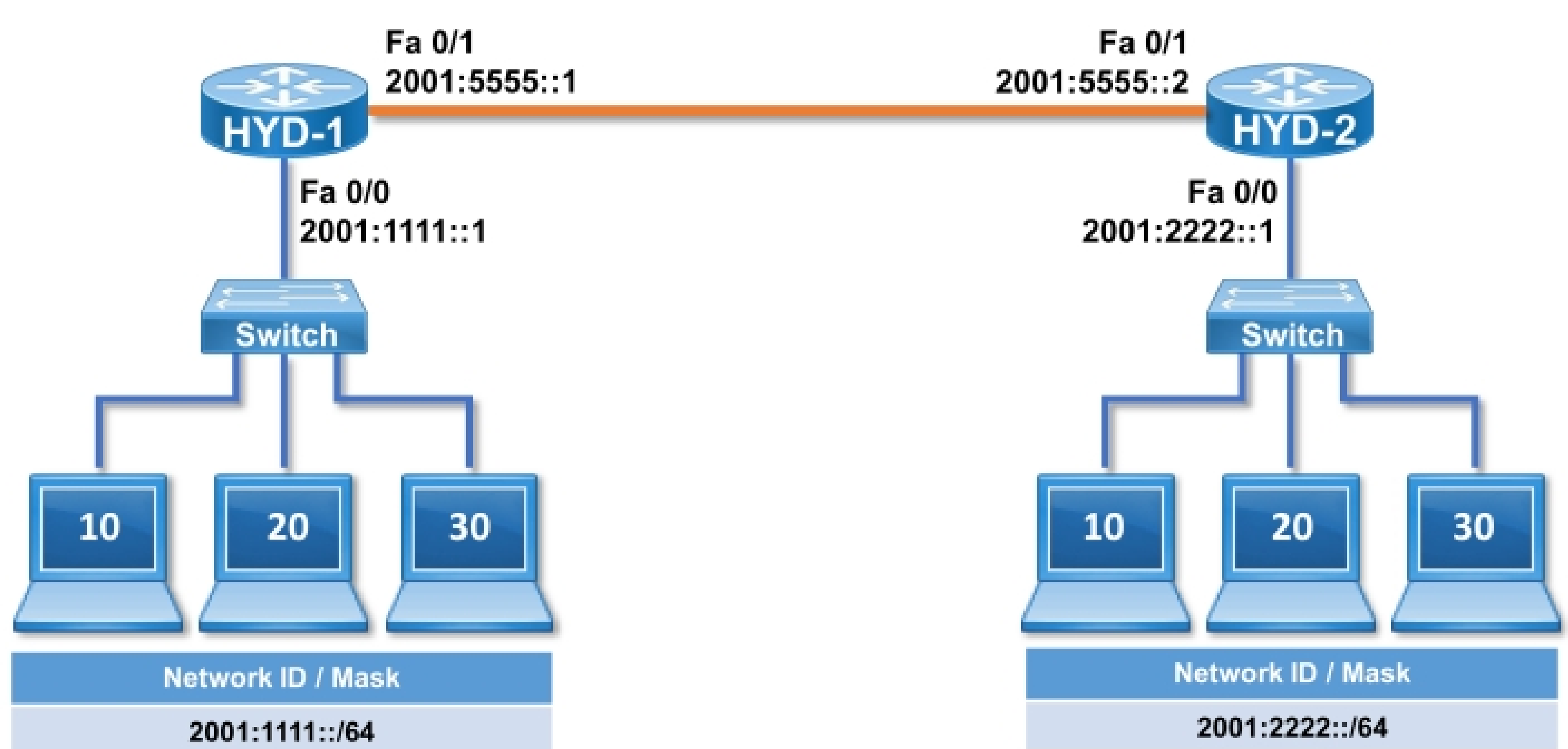
Router (config-ipv6-acl) # <permit/deny> <protocol>
<IPv6 source address> <prefix length>
< IPv6 destination address> <prefix length>
<operator> <service>

Implementation of IPv6 Access List

Router (config) # interface <interface type> <interface no>

Router (config-if) # ipv6 traffic-filter <acl name> <out/in>

IPv6 ACL - Configuration



2001:1111::10/128 should not access 2001:1111::10/128 Host (Web service)

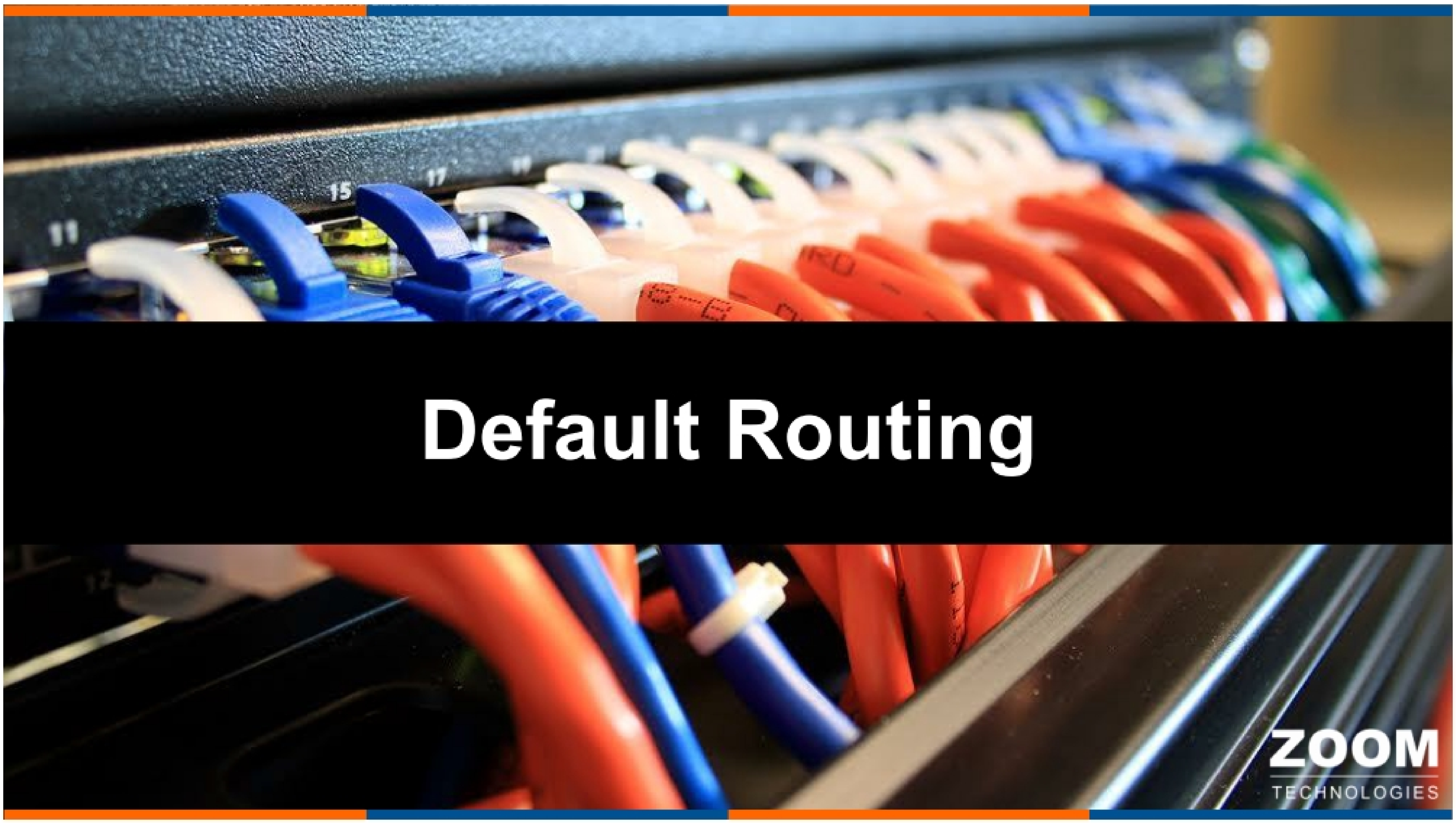
IPv6 ACL - Configuration

HYD-1

```
HYD-1 # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HYD-1 (config) # ipv6 access-list cisco
HYD-1 (config-ipv6-acl) # deny tcp 2001:1111::10/128 2001:2222::10/128 eq 80
HYD-1 (config-ipv6-acl) # permit ipv6 any any
HYD-1(config-ipv6-acl) # exit
HYD-1 (config) #

HYD-1 (config) # interface FastEthernet 0/0
HYD-1 (config-if) # ipv6 traffic-filter cisco in
HYD-1 (config-if) # exit
HYD-1 (config)#
```

IPv6 ACL - Named - Configuration

Router # show ip access-lists



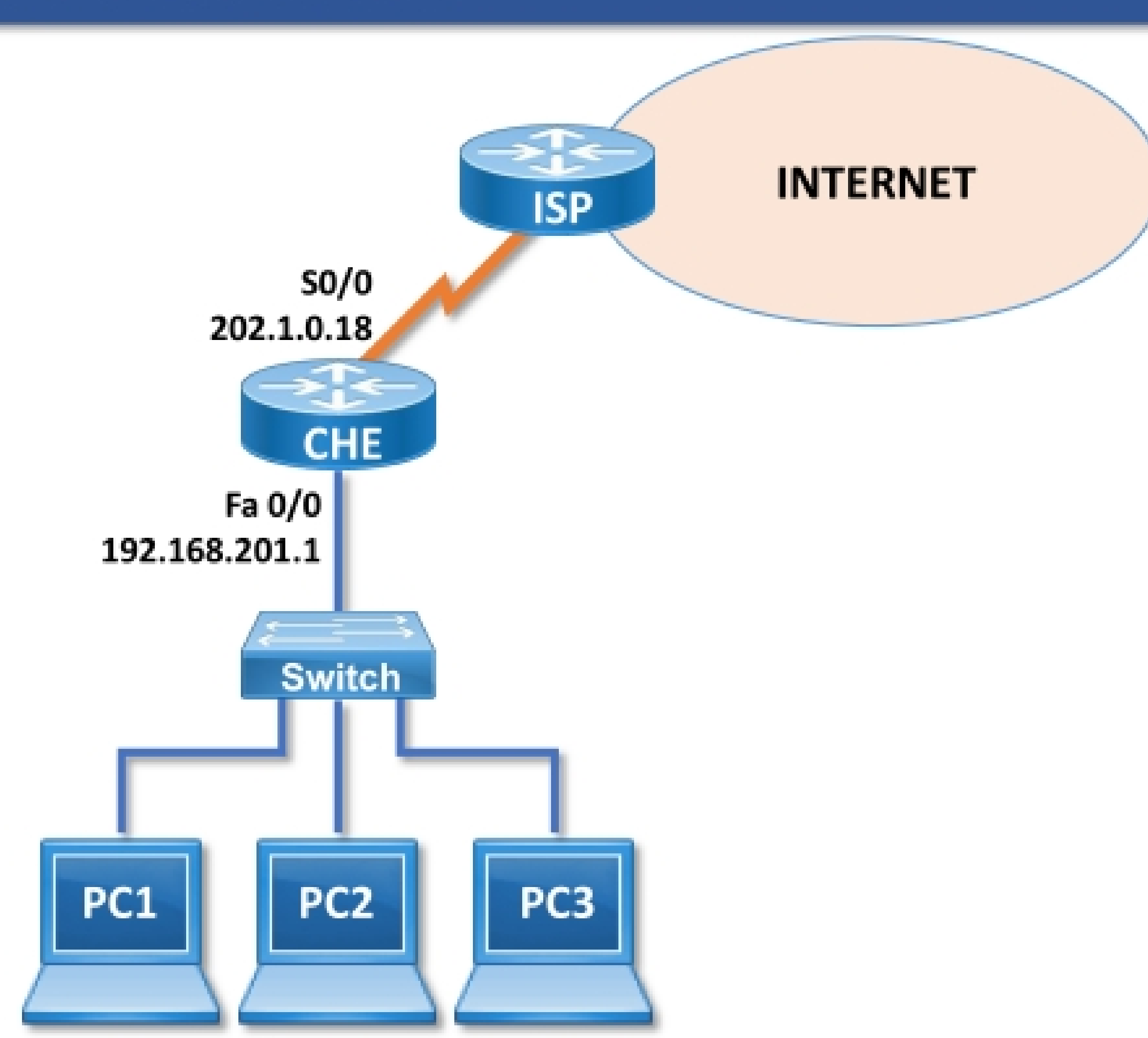
Default Routing

- A default route or gateway of last resort, allows traffic to be forwarded, even without a specific route to a particular network.
- The default route is identified by all zeros in both the network and subnet mask (0.0.0.0   0.0.0.0)
- It is generally configured for accessing Internet, where destination is unknown.
- It is the least preferred route in the routing table.

Default Routing on IPv4 Network - Configuration

Router (config) # ip route < Destination Network ID >
< Destination Subnet Mask > < Exit Interface Type >
< Exit Interface No. >

Default Routing on IPv4 Network



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

Default Routing on IPv4 Network - Configuration


```
CHE # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CHE (config) # interface serial 0/0
CHE (config-if) # ip address 202.1.0.18 255.255.255.248
CHE (config-if) # no shutdown
CHE (config-if) # encapsulation ppp
CHE (config-if) # exit
CHE (config) #
CHE (config) #  ip route 0.0.0.0 0.0.0.0 Serial0/0
```

Default Routing on IPv4 Network - Verification

```
Router #  show ip route
```

NAT

- NAT is a process of changing one IP into another
- NAT is used to save precious public IP addresses.
- NAT is usually used to translate private IP addresses to public IP addresses and vice versa
- It provides security
- Types of NAT
  - Static (one to one mapping)
  - PAT (many to one mapping)

Private IP Address

- There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.
- These addresses are not Routable (or) valid on Internet.

Class A
10.0.0.0 to 10.255.255.255

Class B
172.16.0.0 to 172.31.255.255

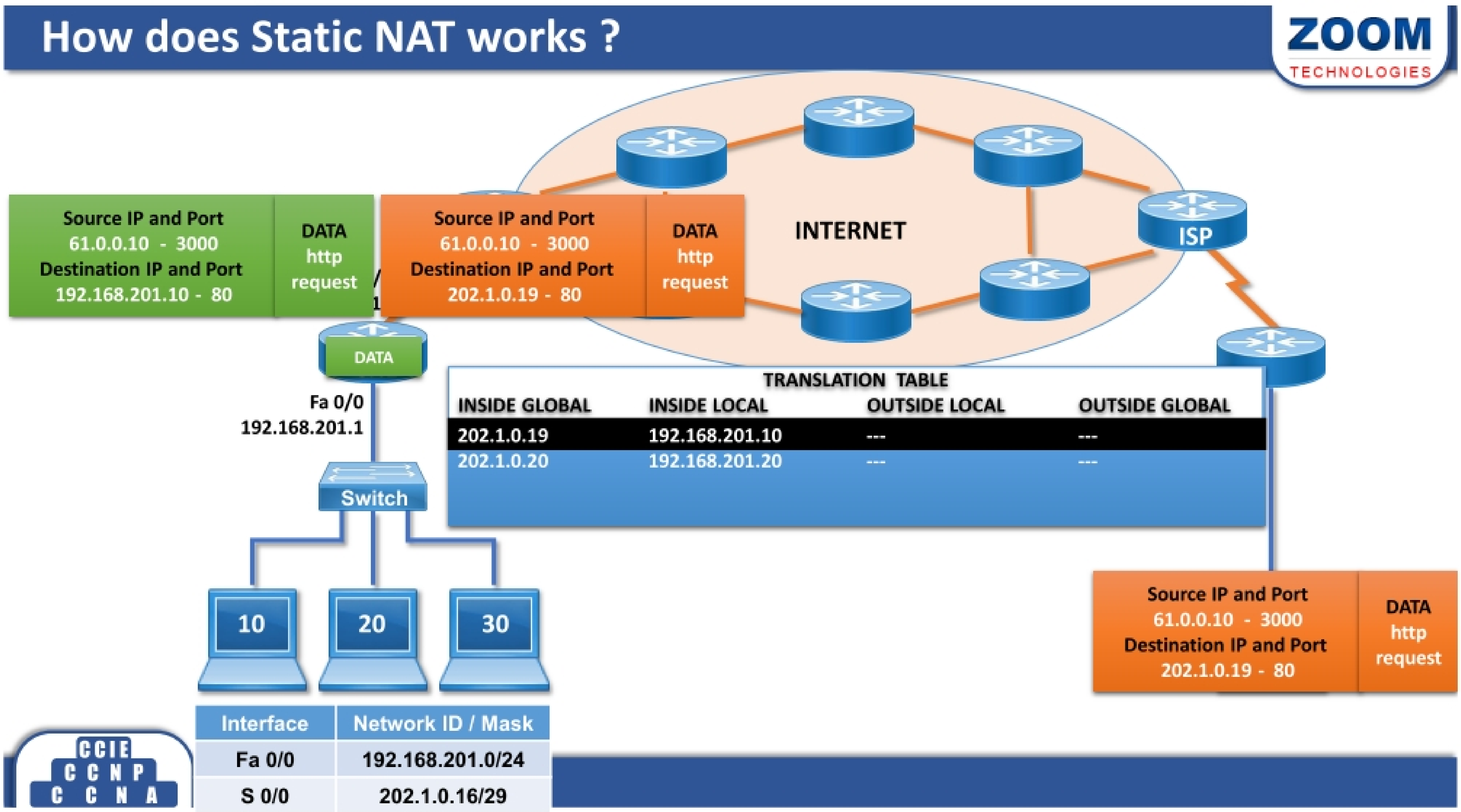
Class C
192.168.0.0 to 192.168.255.255

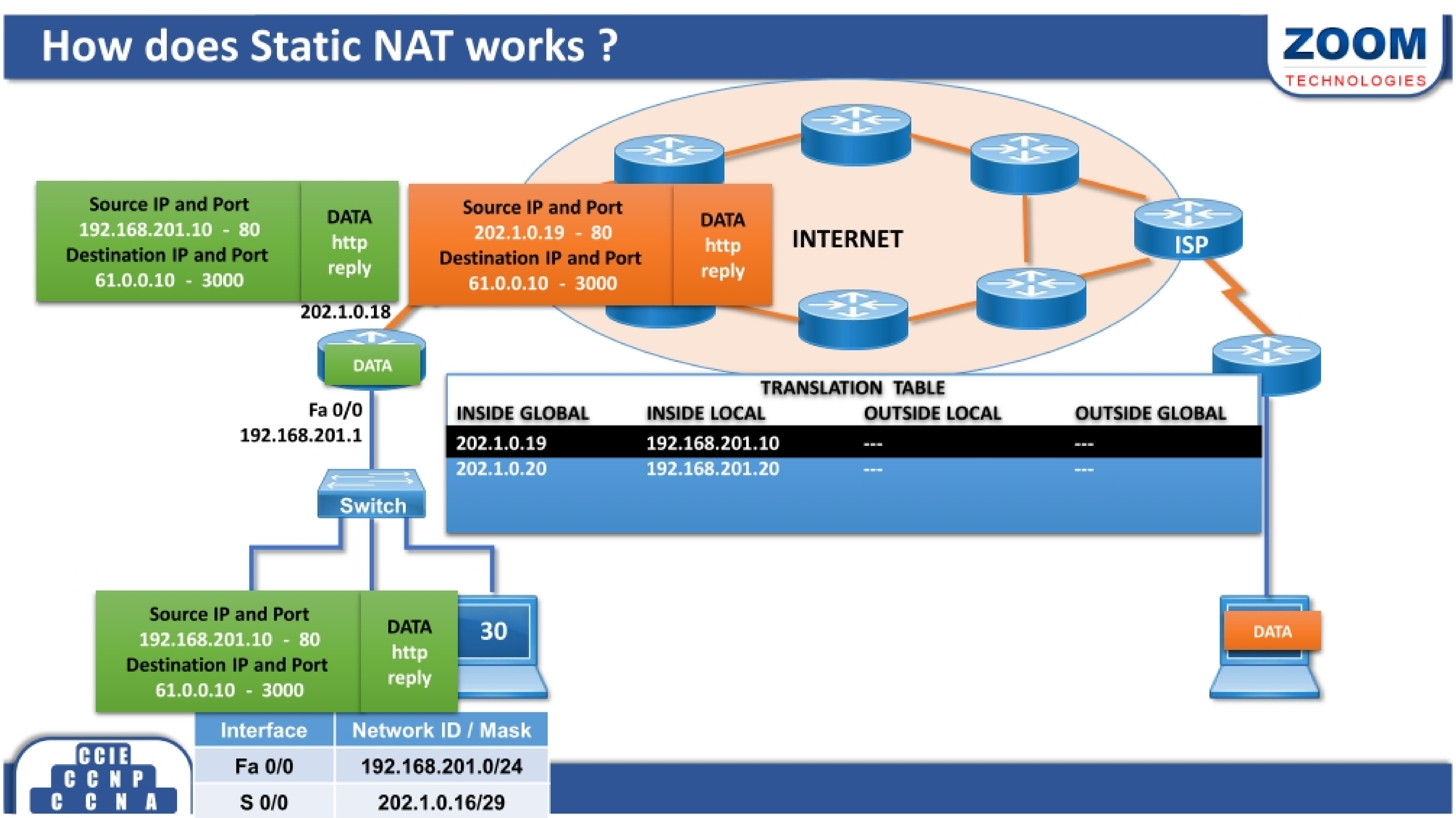
Public IP Address v/s Private IP Address

Public IP Address	Private IP Address
• Used on the Internet (i.e. Public Network) • It should be unique over the Internet. • Assigned by the Internet Service Provider. • Need to purchased from Internet Service Provider.	• Used within the Organization (i.e. Private Network or LAN) • It should be unique within the LAN or Organization • Assigned by Network Administrator • FREE

Static NAT

- One private IP address is mapped to one public IP address.
- Generally used for hosting public servers. (Internet to Server)
- Generally configured for inbound traffic.


How does Static NAT works ?
Source IP and Port
61.0.0.10 - 3000
Destination IP and Port
192.168.201.10 - 80
DATA
http
request
Source IP and Port
61.0.0.10 - 3000
Destination IP and Port
202.1.0.19 - 80
DATA
http
request
INTERNET
ISP
DATA
Fa 0/0
192.168.201.1
Switch
10
20
30
TRANSLATION TABLE
INSIDE GLOBAL | INSIDE LOCAL | OUTSIDE LOCAL | OUTSIDE GLOBAL
202.1.0.19 | 192.168.201.10 | --- | ---
202.1.0.20 | 192.168.201.20 | --- | ---
Source IP and Port
61.0.0.10 - 3000
Destination IP and Port
202.1.0.19 - 80
DATA
http
request
Interface | Network ID / Mask
Fa 0/0 | 192.168.201.0/24
S 0/0 | 202.1.0.16/29


How does Static NAT works ?
Source IP and Port
192.168.201.10 - 80
Destination IP and Port
61.0.0.10 - 3000
DATA
http
reply
Source IP and Port
202.1.0.19 - 80
Destination IP and Port
61.0.0.10 - 3000
DATA
http
reply
INTERNET
ISP
202.1.0.18
DATA
Fa 0/0
192.168.201.1
Switch
TRANSLATION TABLE
INSIDE GLOBAL | INSIDE LOCAL | OUTSIDE LOCAL | OUTSIDE GLOBAL
202.1.0.19 | 192.168.201.10 | --- | ---
202.1.0.20 | 192.168.201.20 | --- | ---
Source IP and Port
192.168.201.10 - 80
Destination IP and Port
61.0.0.10 - 3000
DATA
http
reply
30
DATA
Interface | Network ID / Mask
Fa 0/0 | 192.168.201.0/24
S 0/0 | 202.1.0.16/29

Static NAT - Configuration

Defining NAT on Interfaces

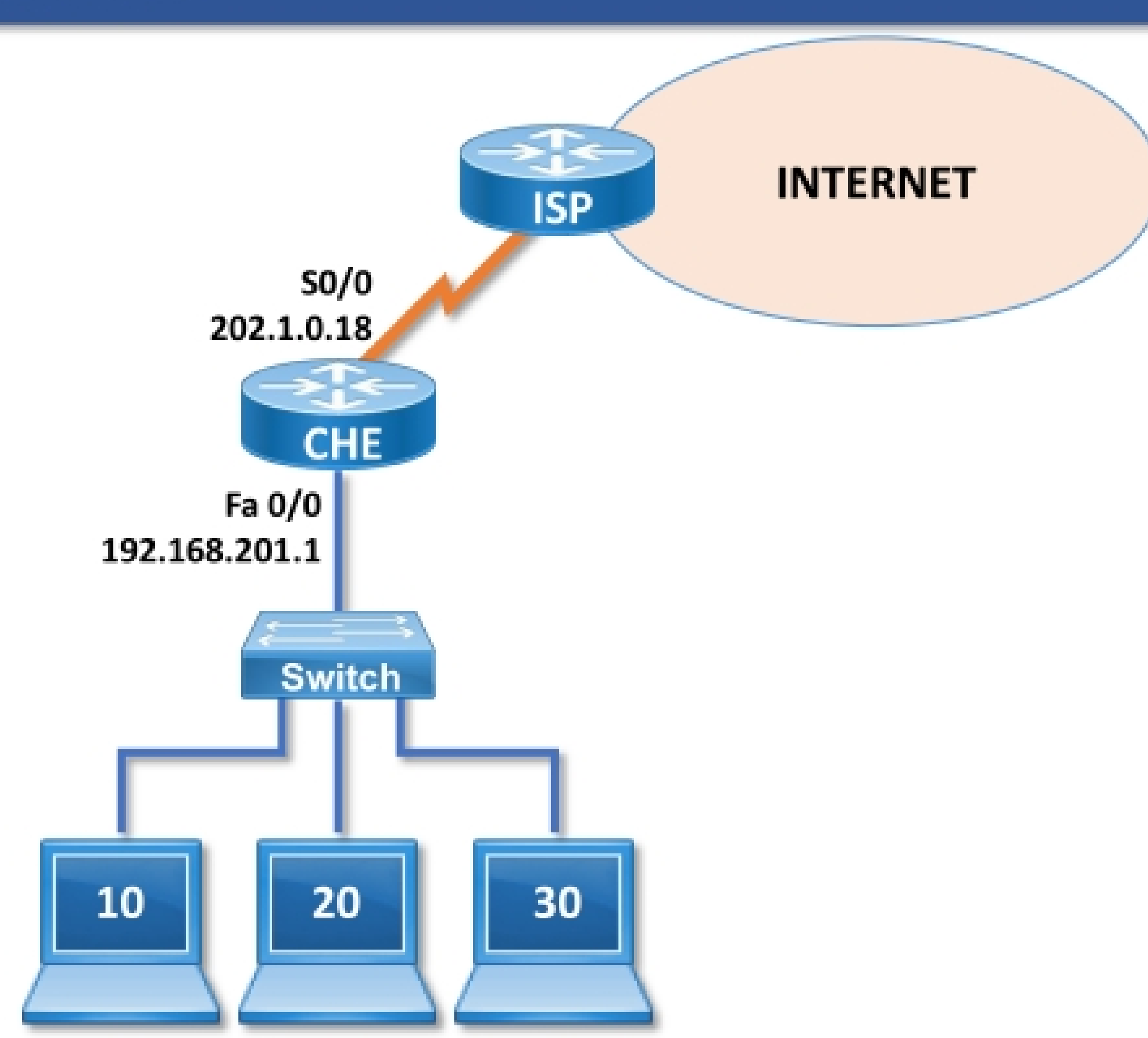
Router (config) # interface <interface type> <interface number>

Router (config-if) # ip nat inside/outside

Configuring static NAT

Router (config) # ip nat inside source static <private ip> <public ip>

Static NAT - Configuration



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

Static NAT - Configuration


```
CHE # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CHE (config) # interface serial 0/0
CHE (config-if) # ip nat outside
CHE (config-if) # exit
CHE (config) # interface FastEthernet 0/0
CHE (config-if) # ip nat inside
CHE (config-if) # exit
CHE (config)# ip nat inside source static 192.168.201.10 202.1.0.19
```

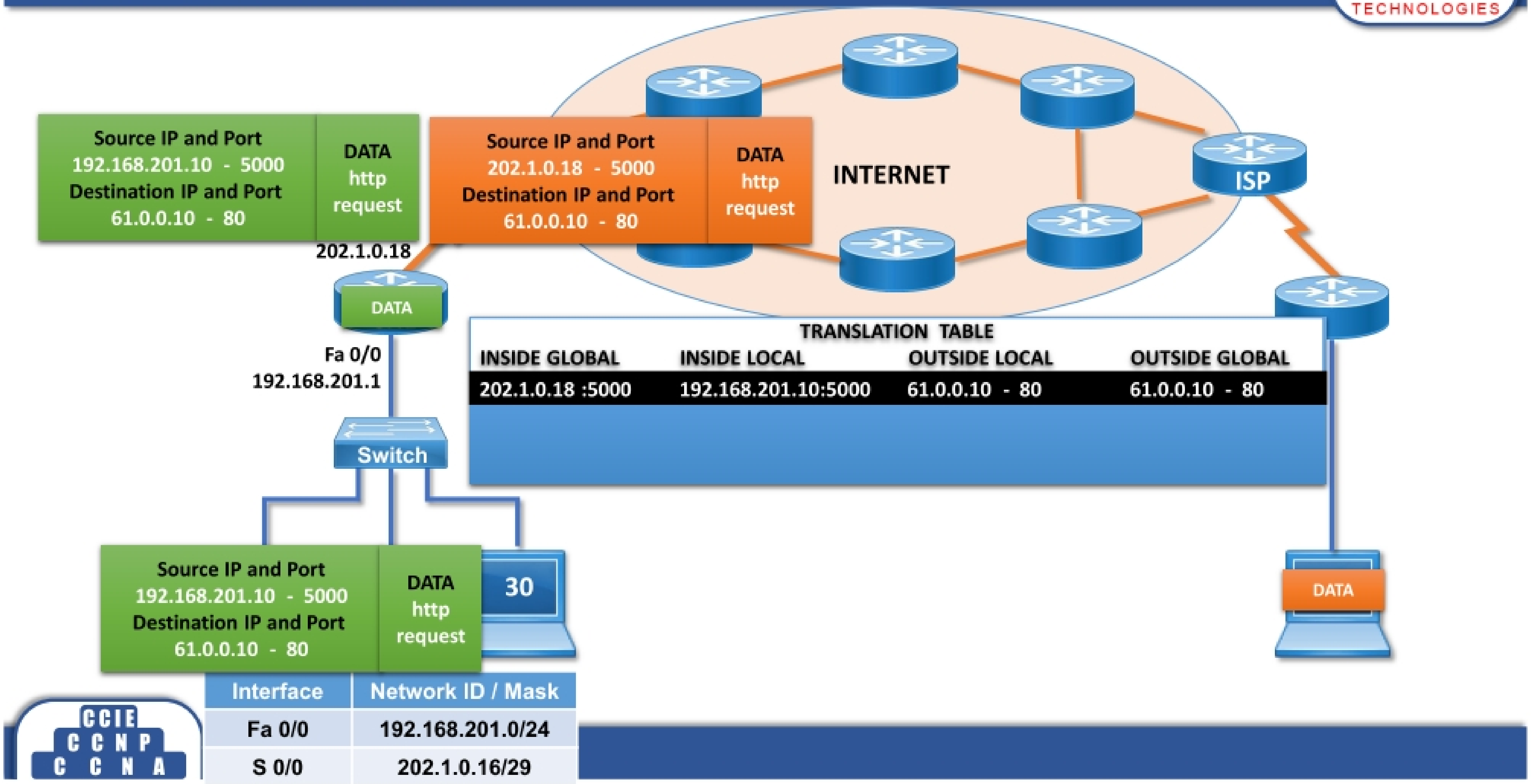
Static NAT - Verification

```
Router #  show ip nat translations
```

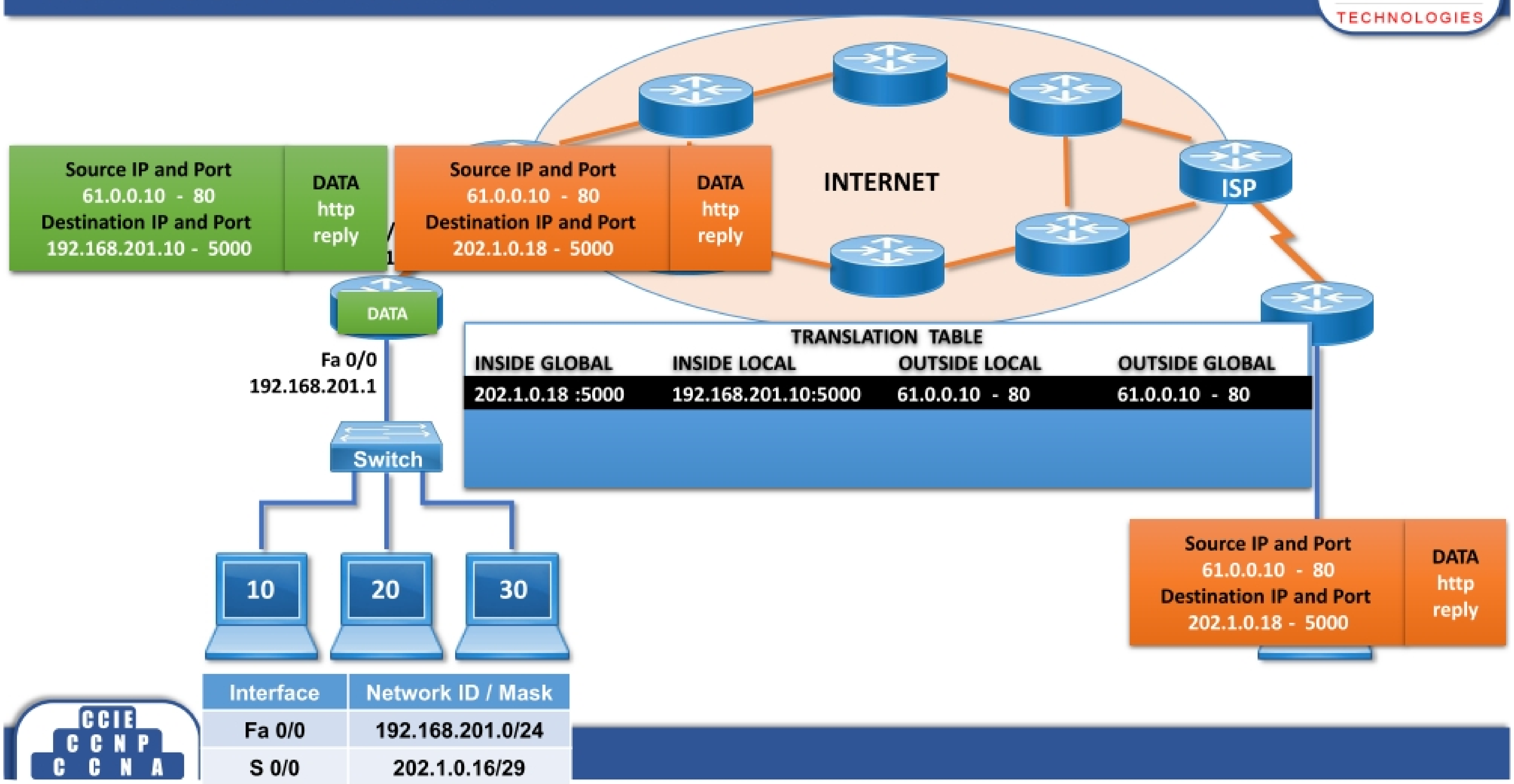
PAT (Overloading)

- Many private IP addresses are mapped to one public IP address.
- Configured for outbound traffic (LAN to Internet)
- All users can access Internet at the same time.

How does PAT works ?

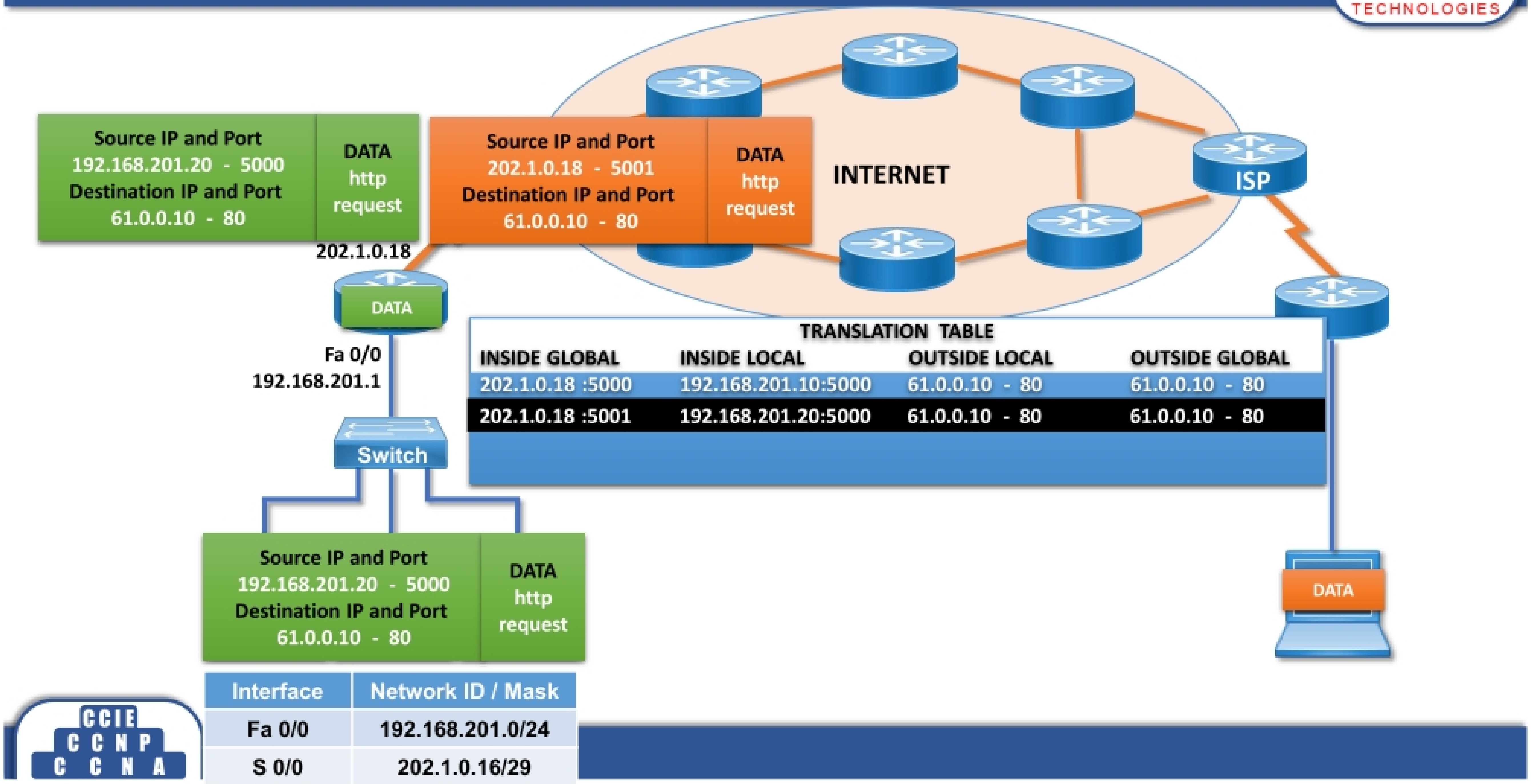


How does PAT works ?



How does PAT works ?

ZOOM TECHNOLOGIES



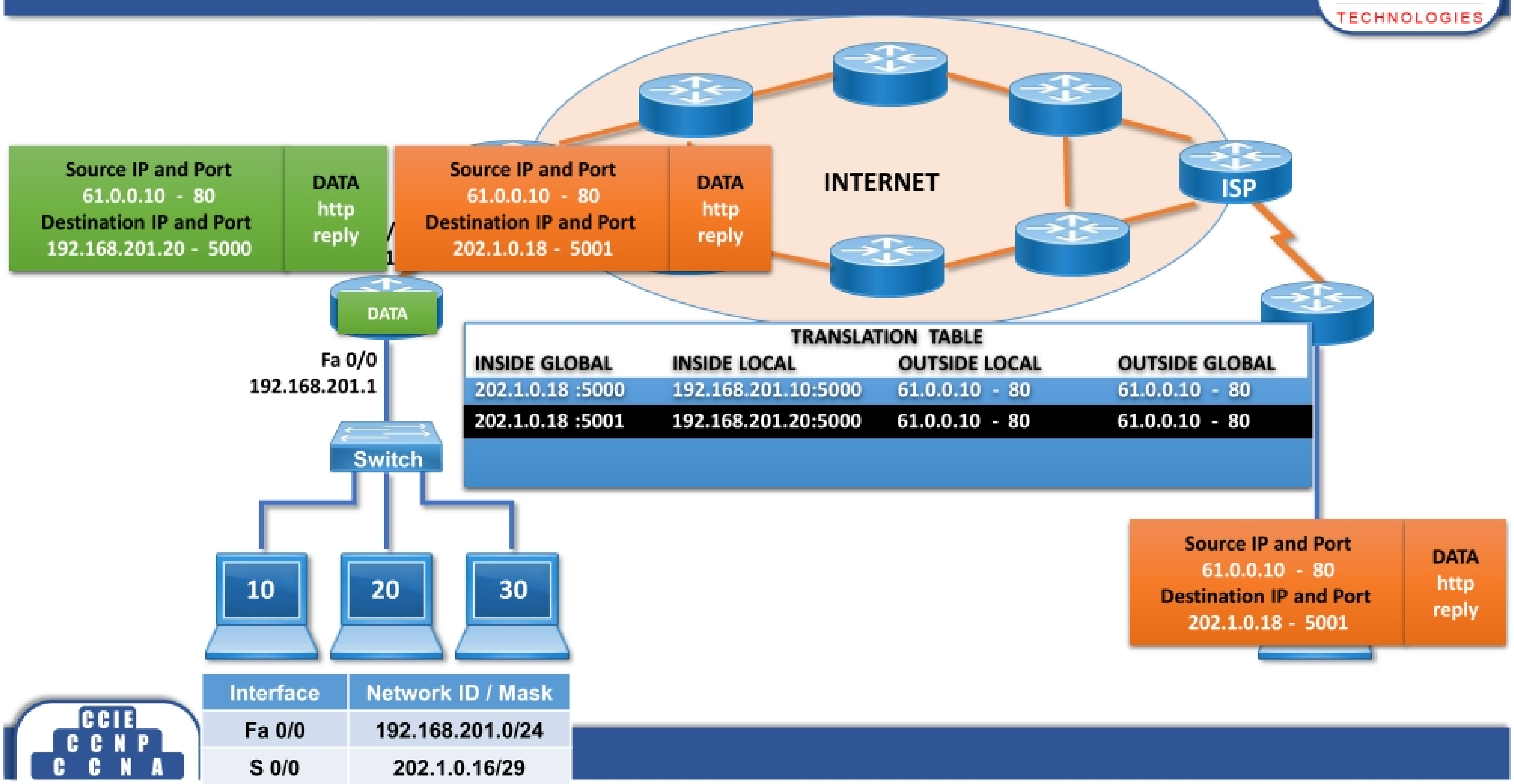
TRANSLATION TABLE

INSIDE GLOBAL	INSIDE LOCAL	OUTSIDE LOCAL	OUTSIDE GLOBAL
202.1.0.18 :5000	192.168.201.10:5000	61.0.0.10 - 80	61.0.0.10 - 80
202.1.0.18 :5001	192.168.201.20:5000	61.0.0.10 - 80	61.0.0.10 - 80

Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

How does PAT works ?

ZOOM TECHNOLOGIES



TRANSLATION TABLE

INSIDE GLOBAL	INSIDE LOCAL	OUTSIDE LOCAL	OUTSIDE GLOBAL
202.1.0.18 :5000	192.168.201.10:5000	61.0.0.10 - 80	61.0.0.10 - 80
202.1.0.18 :5001	192.168.201.20:5000	61.0.0.10 - 80	61.0.0.10 - 80

Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

PAT - Configuration

Defining NAT on Interfaces

Router (config) # interface <interface type> <interface number>

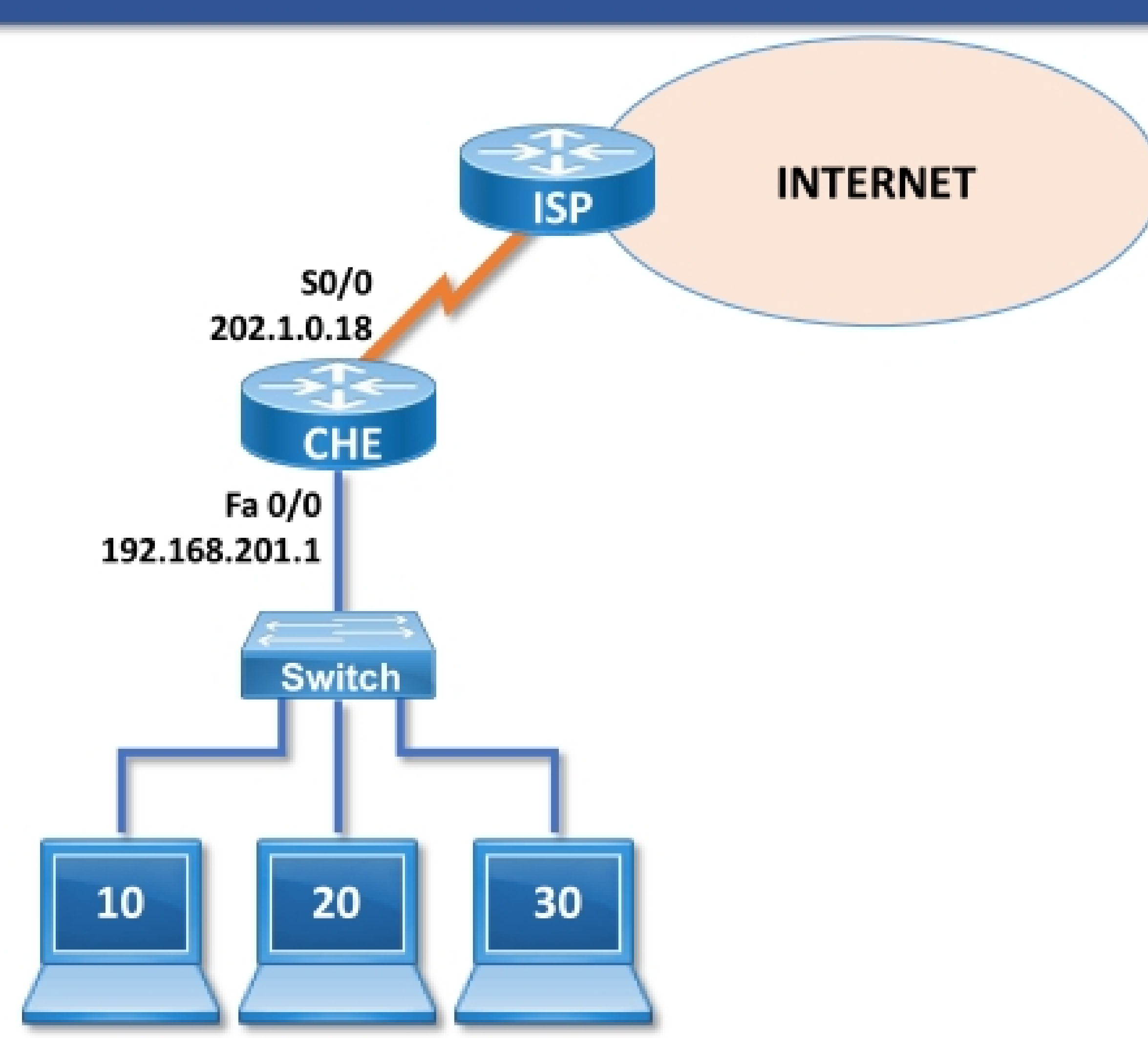
Router (config-if) # ip nat inside/outside

Configuring PAT

Router (config) # ip nat inside source list <acl no.> interface

< interface type > < interface no. > overload

PAT - Configuration



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

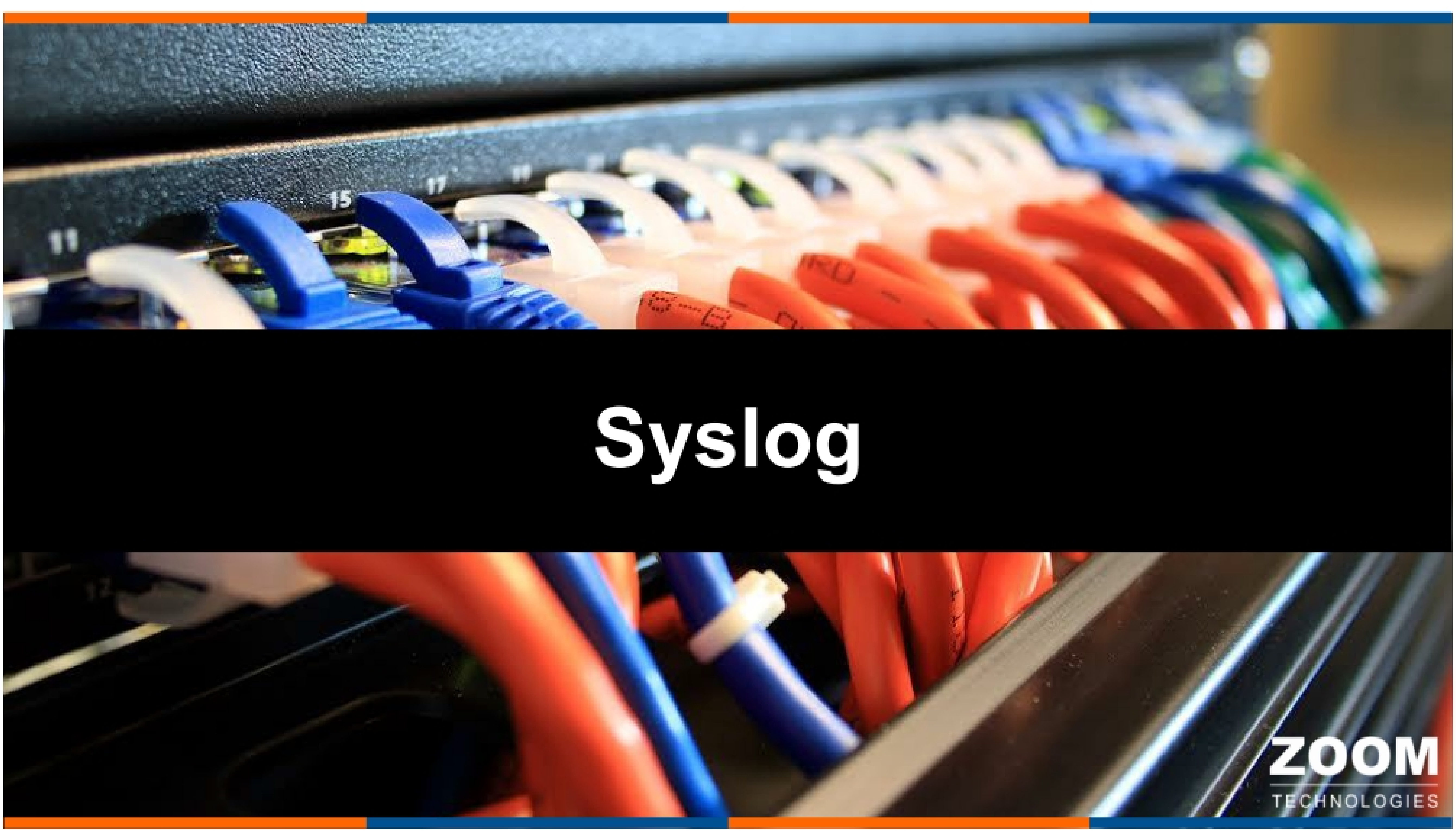
PAT - Configuration

CHE # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CHE (config) # interface serial 0/0
CHE (config-if) # ip nat outside
CHE (config-if) # exit
CHE (config) # interface FastEthernet 0/0
CHE (config-if) # ip nat inside
CHE (config-if) # exit
CHE (config) # access-list 10 permit 192.168.201.0 0.0.0.255
CHE (config) # ip nat inside source list 10 interface serial 0/0 overload

PAT - Verification

Router # show ip nat translations


Network Services
ZOOM
TECHNOLOGIES


Syslog
ZOOM
TECHNOLOGIES

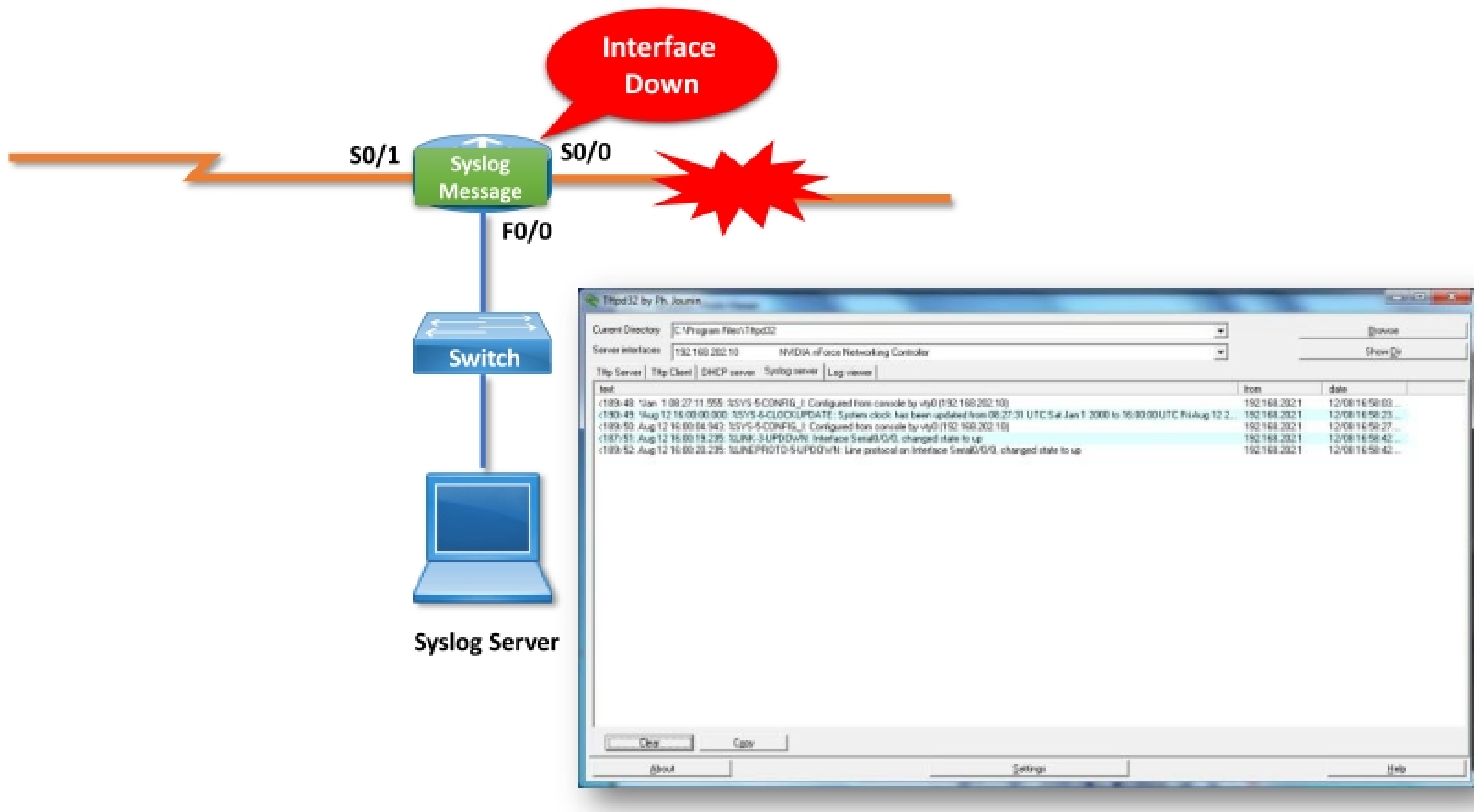
Syslog

- Syslog is a protocol that allows a network device to send their system messages/notification across the network to message collectors
- Syslog is typically used for network management and security auditing.
- Syslog uses the UDP port number 514.
- Device can be configured to forward syslog messages to various destination
  - Buffer : send syslog messages to internal memory buffer
  - Syslog Server : send syslog messages to syslog server

Message Severity Levels

Level	Level Name	Explanation
0	Emergency	The System may be unusable
1	Alert	Immediate action may be required
2	Critical	A critical event took place
3	Error	A router experienced an error
4	warning	A condition might warrant attention
5	Notification	A normal but significant condition occurred
6	Informational	A normal event occurred
7	Debugging	The output is a result of a debug command

How Syslog Works ?



Syslog Message Format

Timestamp	Severity Level	Description
Sep 22 2016 15:24:53.080 :	%LINK-5-CHANGED:	Interface Serial 0/0, changed state to administratively down

Logging to Buffer - Configuration

Router (config) # logging on

Router (config) # logging buffered <level>

Logging to Syslog Server - Configuration

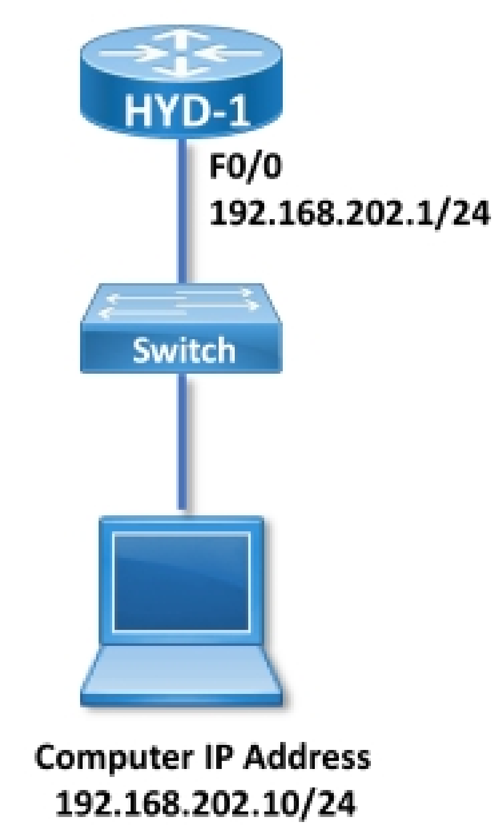
Router (config) # logging on

Router (config) # logging host <server ip address>

Router (config) # logging trap <level>

Router (config) # service timestamps log datetime msec

Logging to Syslog Server - Configuration



Logging to Syslog Server - Configuration

HYD-1

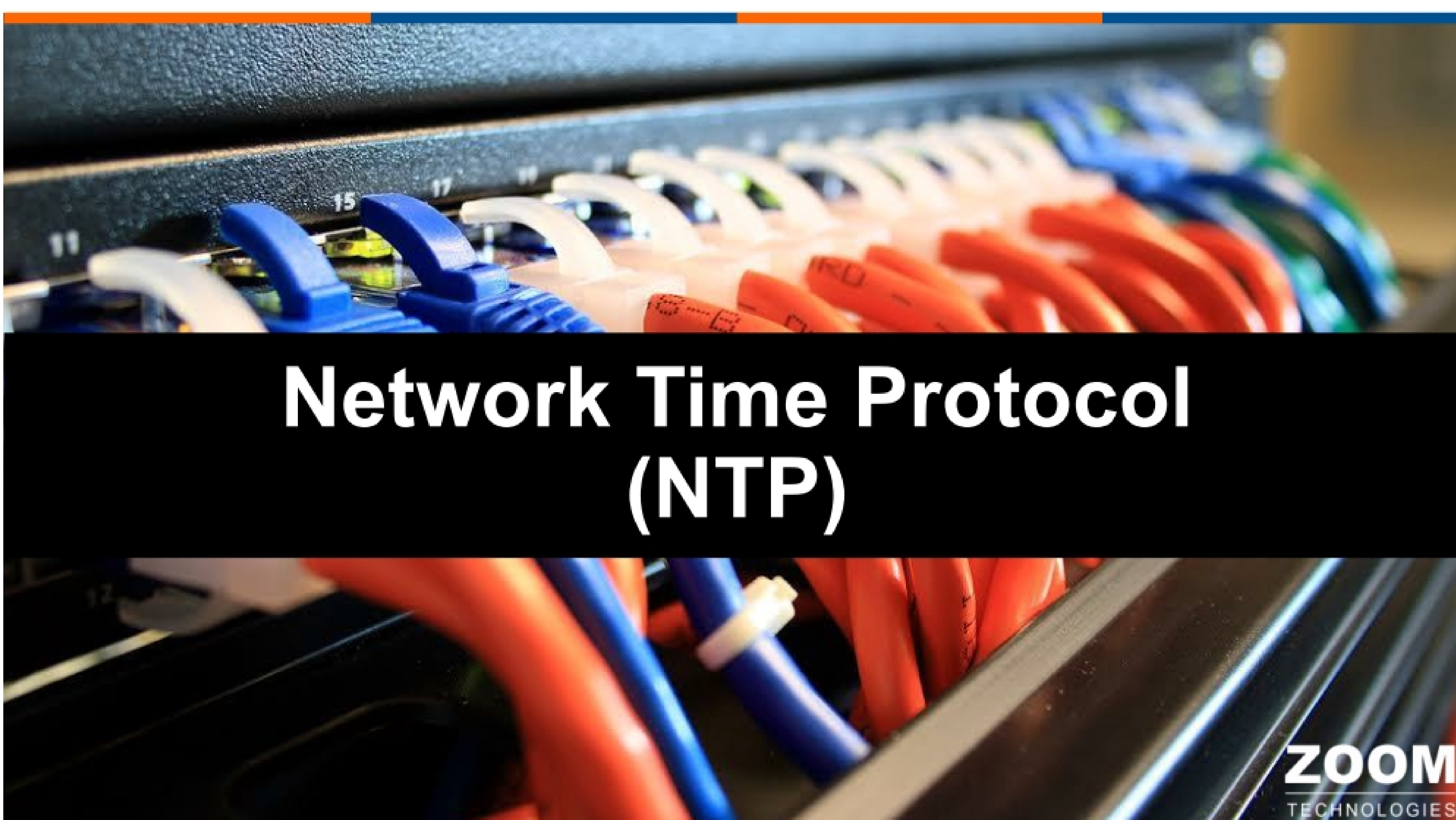
HYD-1 (config) # logging on
HYD-1 (config) # logging host 192.168.202.10
HYD-1 (config) # logging trap 7
HYD-1 (config) # service timestamps log datetime msec

HYD-1

HYD-1 (config) # logging on
HYD-1 (config) # logging buffered 7

Logging to Syslog Server – Verification

Router # show logging



Manual Clock

- Manually setting the clocks of network device is neither accurate nor scalable.
- The best practice is to use Network Time Protocol (NTP)

Date and Time - Configuration

```
Router #   clock set  <hh:mm:ss>  <dd mm yyyy>
```

Date and Time - Verification

Router # show clock

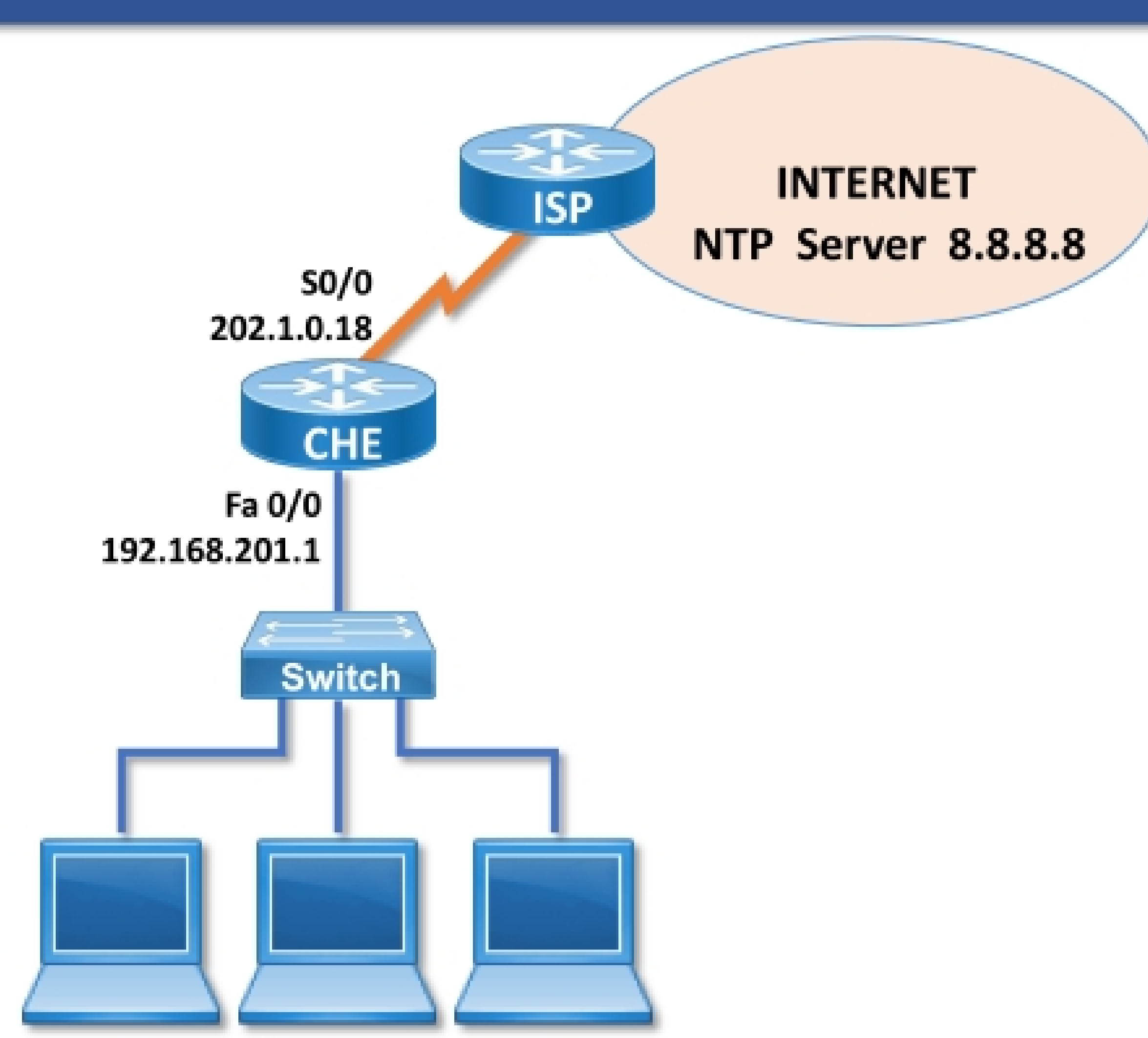
Network Time Protocol (NTP)

- NTP (Network Time Protocol) is used to synchronize the time throughout network devices i.e. servers, switches, routers, wireless access points, etc. to synchronize their clocks with a central source clock.
- NTP works on UDP port 123 for both the source and destination by default.
- NTP can get correct time from internal and external source.
- Normally a router or switch will run in NTP client mode which means that it will adjust its clock based on the time of a NTP server.

NTP - Configuration

Router (config) # ntp server <server ip address>

NTP - Configuration



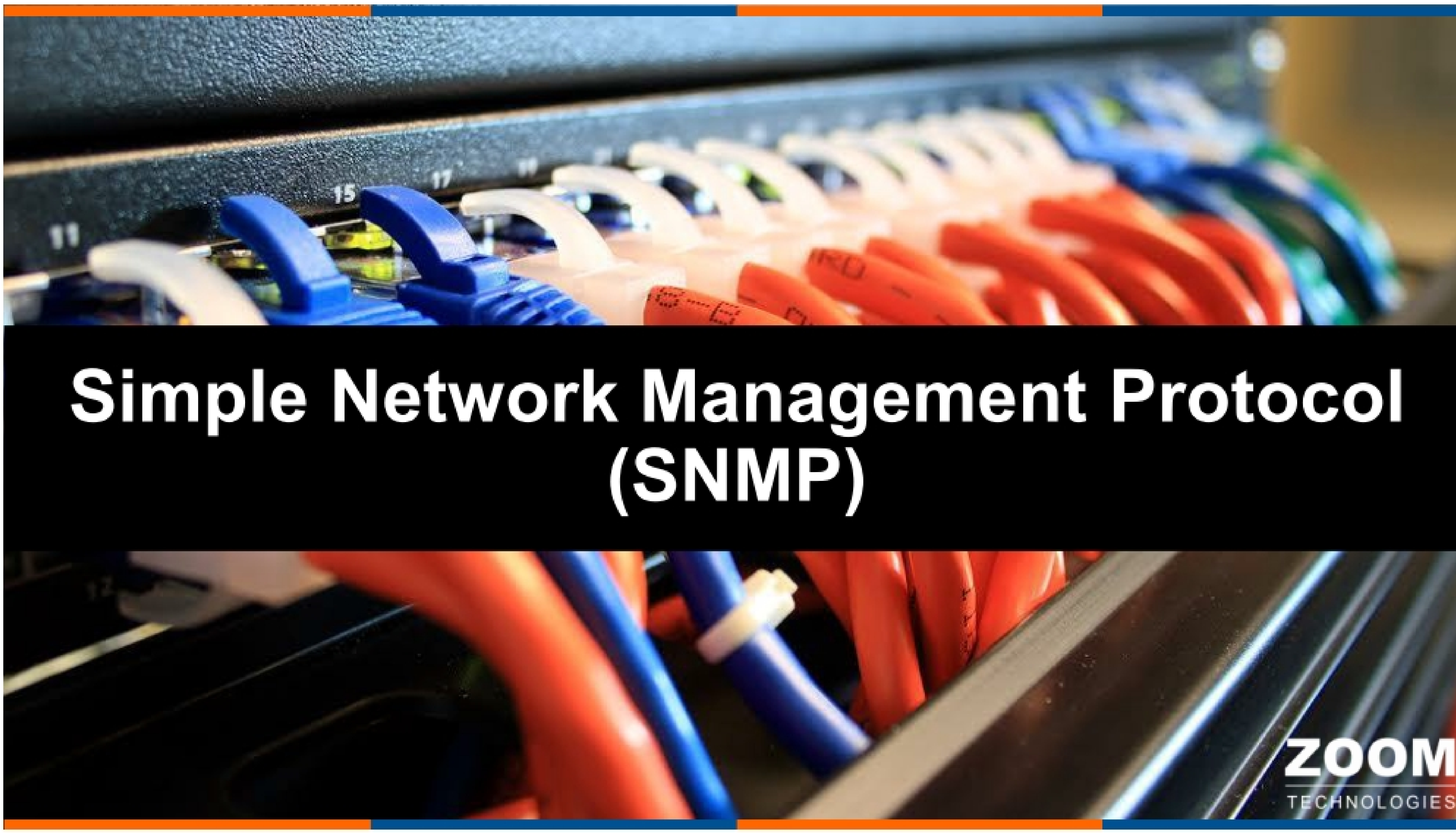
Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

NTP - Configuration

```
CHE # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CHE (config) # ntp server 8.8.8.8
CHE (config) # exit
```

NTP – Verification

Router # show clock
Router # show ntp associations
Router # show ntp status



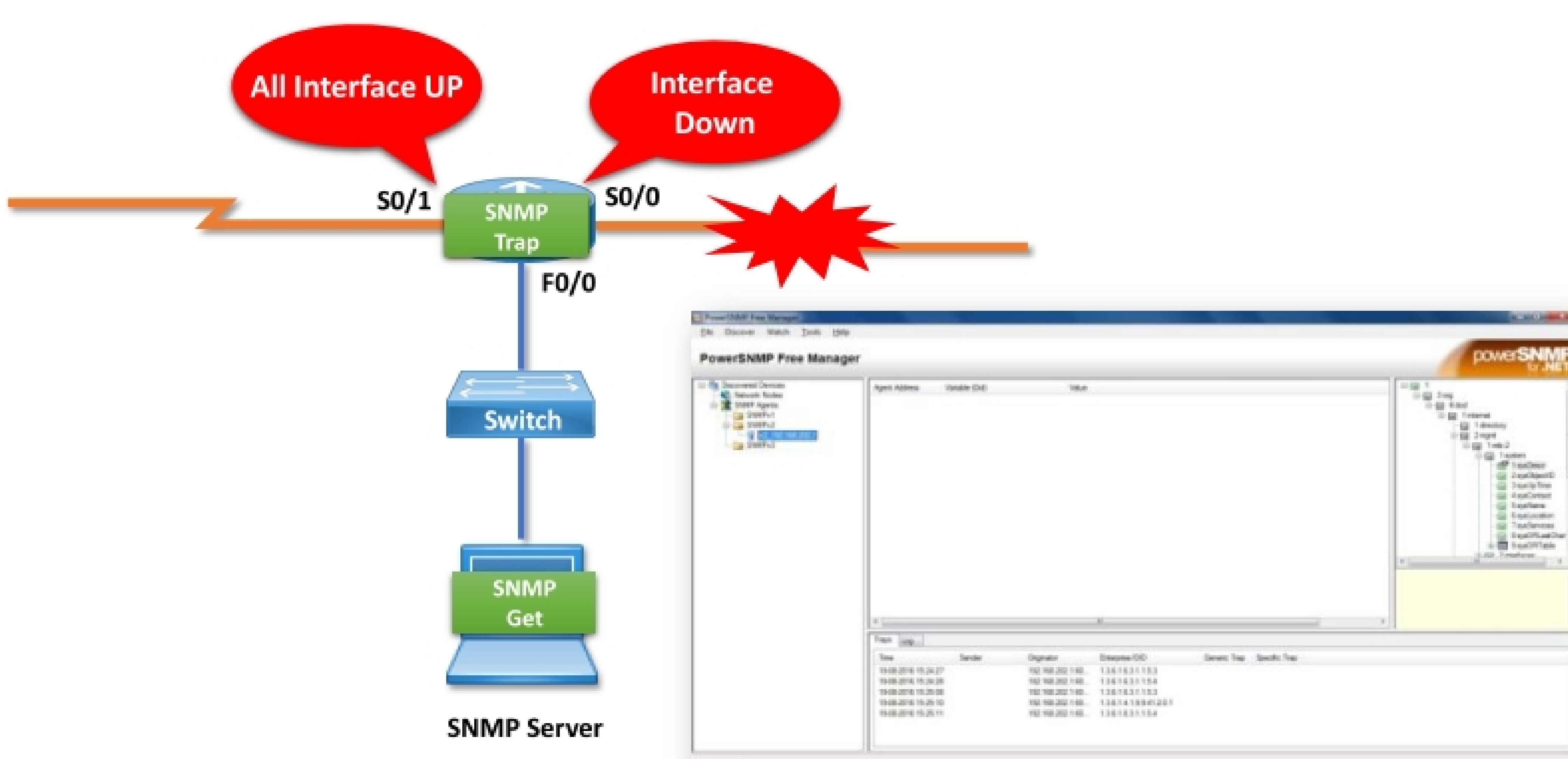
SNMP

- SNMP is an application layer protocol, uses the UDP port number 161.
- It provides a message format for communication between Network Devices (Agents) and Network Manager.

SNMP Components

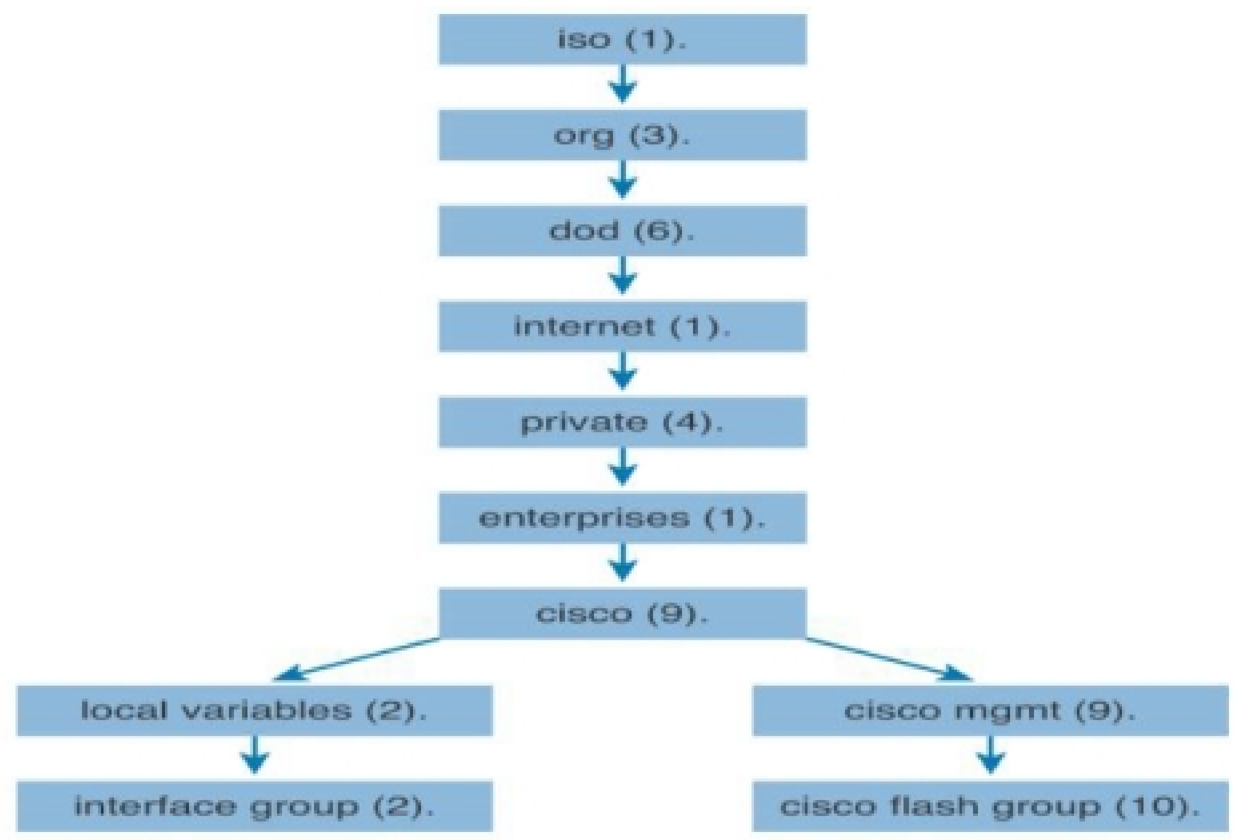
- SNMP Managers
  - It is software that collects information from network devices (i.e. NMS)
- SNMP Agents
  - SNMP enabled network devices i.e. Router, Switch, Server, etc.
- Management Information Base:
  - Contains the database of objects (information variables)

How SNMP Works ?



Management Information Base

- MIB defines each variable as object id (OID).
- Organizes that into a hierarchy of OIDs, usually shown as tree.



SNMP versions

SNMP version	Security	Bulk Retrieval Information
Version 1	Plain authentication with community string	NO
Version 2	Plain authentication with community string	YES
Version 3	Strong authentication, confidentiality and integrity	YES

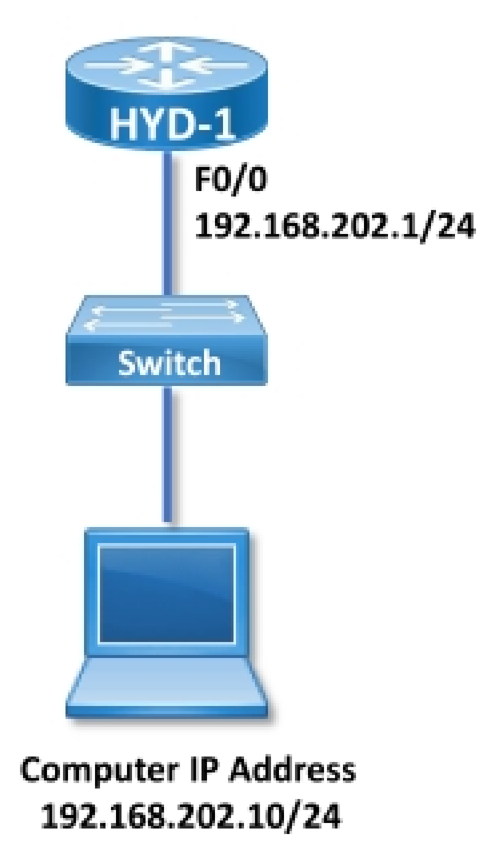
SNMP - Configuration

Router (config) # snmp-server community <string>
< ro | rw >

Router (config) # snmp-server host <server ip address>
version <snmp version> <string>

Router (config) # snmp-server enable traps

SNMP - Configuration



SNMP - Configuration


```
HYD-1 (config) # snmp-server community public rw
HYD-1 (config) # snmp-server host 192.168.202.10 version 2c public
HYD-1 (config) # snmp-server enable traps
HYD-1 (config) # exit
```

SNMP – Verification

```
Router #  show snmp community
Router #  show snmp host
```

Dynamic Host Control Protocol (DHCP)

ZOOM TECHNOLOGIES

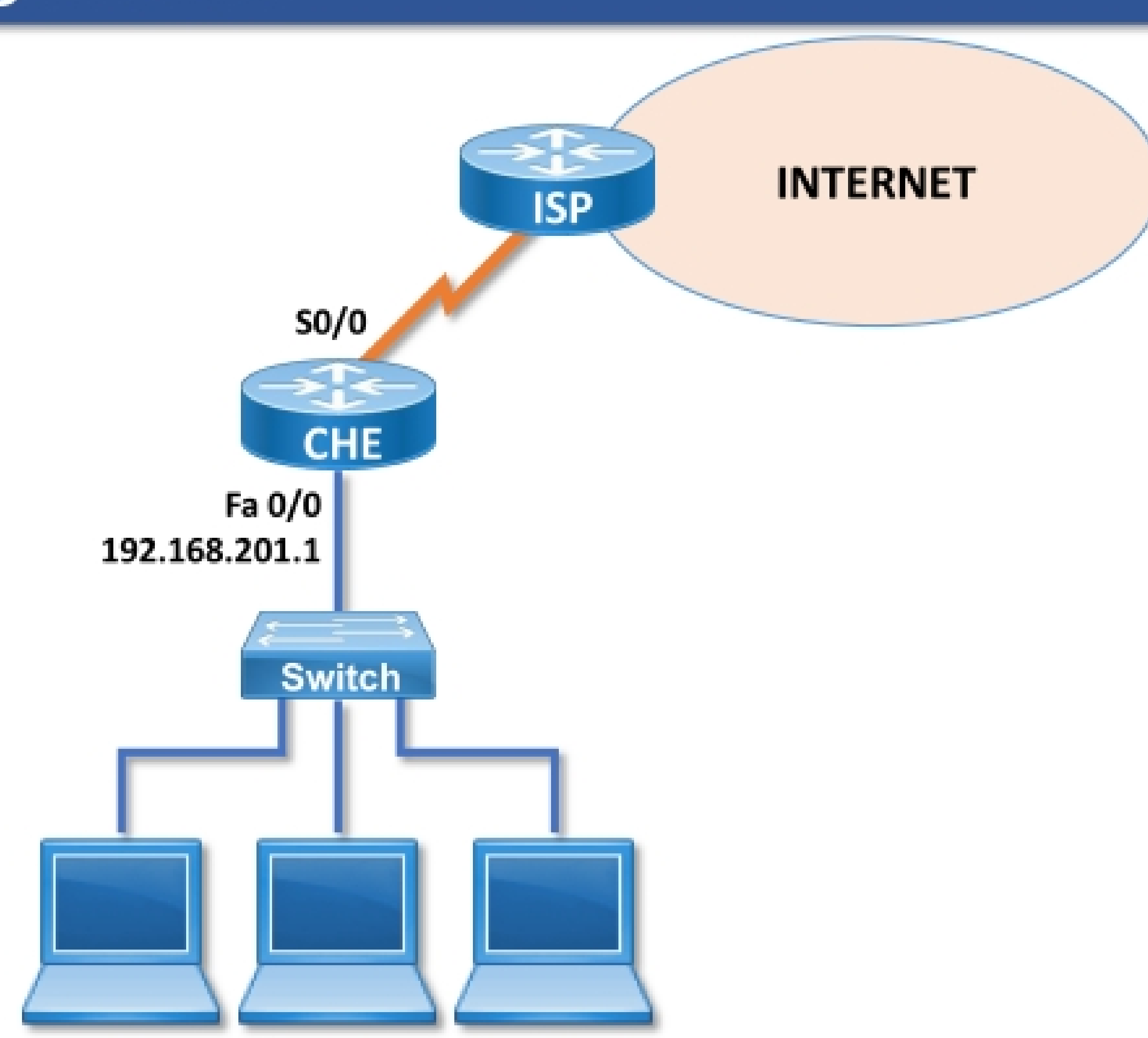
- Dynamic Host Control Protocol is used for dynamic IP address assignment to network devices / hosts.
- DHCP server provides IP address, Subnet mask, Default gateway and DNS server IP address to DHCP clients.
- Router can be configured both as a DHCP Server and DHCP Client.

CCIE CCNP CCNA

DHCP Server - Configuration

Router (config) # ip dhcp pool < name >
Router (dhcp-config) # network < network address > < subnet mask >
Router (dhcp-config) # default-router < router ip address >
Router (dhcp-config) # dns-server < dns server ip address >
Router (dhcp-config) # lease < days > < hours > <minutes>
Router (dhcp-config) # exit
Router (config) # ip dhcp excluded-address <start address> <end address>
Router (config)# exit

DHCP Server - Configuration



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

DHCP Server - Configuration

ZOOM TECHNOLOGIES


```
CHE # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CHE (config) # ip dhcp pool zoom
CHE (dhcp-config) # network 192.168.201.0 255.0.0.0
CHE (dhcp-config) # default-router 192.168.201.1
CHE (dhcp-config) # dns-server 8.8.8.8
CHE (dhcp-config) # lease 1 1 1
CHE (dhcp-config) # exit
CHE (config) # ip dhcp excluded-address 192.168.201.1 192.168.201.50
CHE (config)# exit
```

CCIE CCNP CCNA

DHCP Server – Verification

ZOOM TECHNOLOGIES

Router # show ip dhcp binding

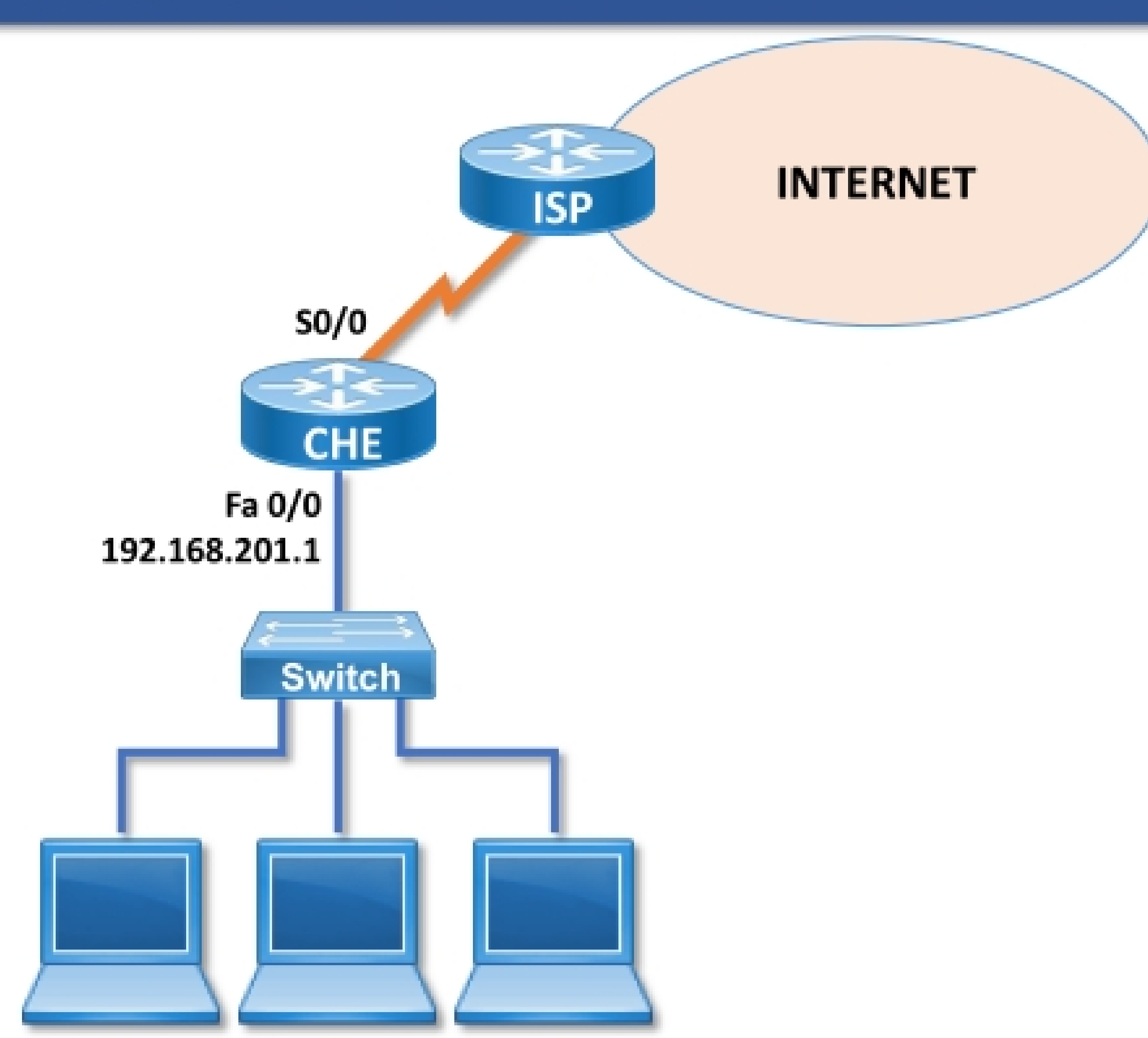
CCIE CCNP CCNA

DHCP Client - Configuration

Router (config) # interface <interface type> <interface no.>
Router (config-if) # ip address dhcp <pool name>
Router (config-if) # no shutdown
Router (config-if) # exit

DHCP Client - Configuration

ZOOM TECHNOLOGIES



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

CCIE CCNP CCNA

DHCP Client - Configuration

```
CHE # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CHE (config)# interface serial 0/0
CHE (config-if)# ip address dhcp zoom
CHE (config-if)# no shutdown
CHE (config-if)# exit
CHE (config)#
```

DHCP Client – Verification

```
Router # show interface <interface type> <interface no>
Router # show ip interface brief
```


Advanced IPv6
ZOOM
TECHNOLOGIES


IPv6 Neighbor Discovery
ZOOM
TECHNOLOGIES

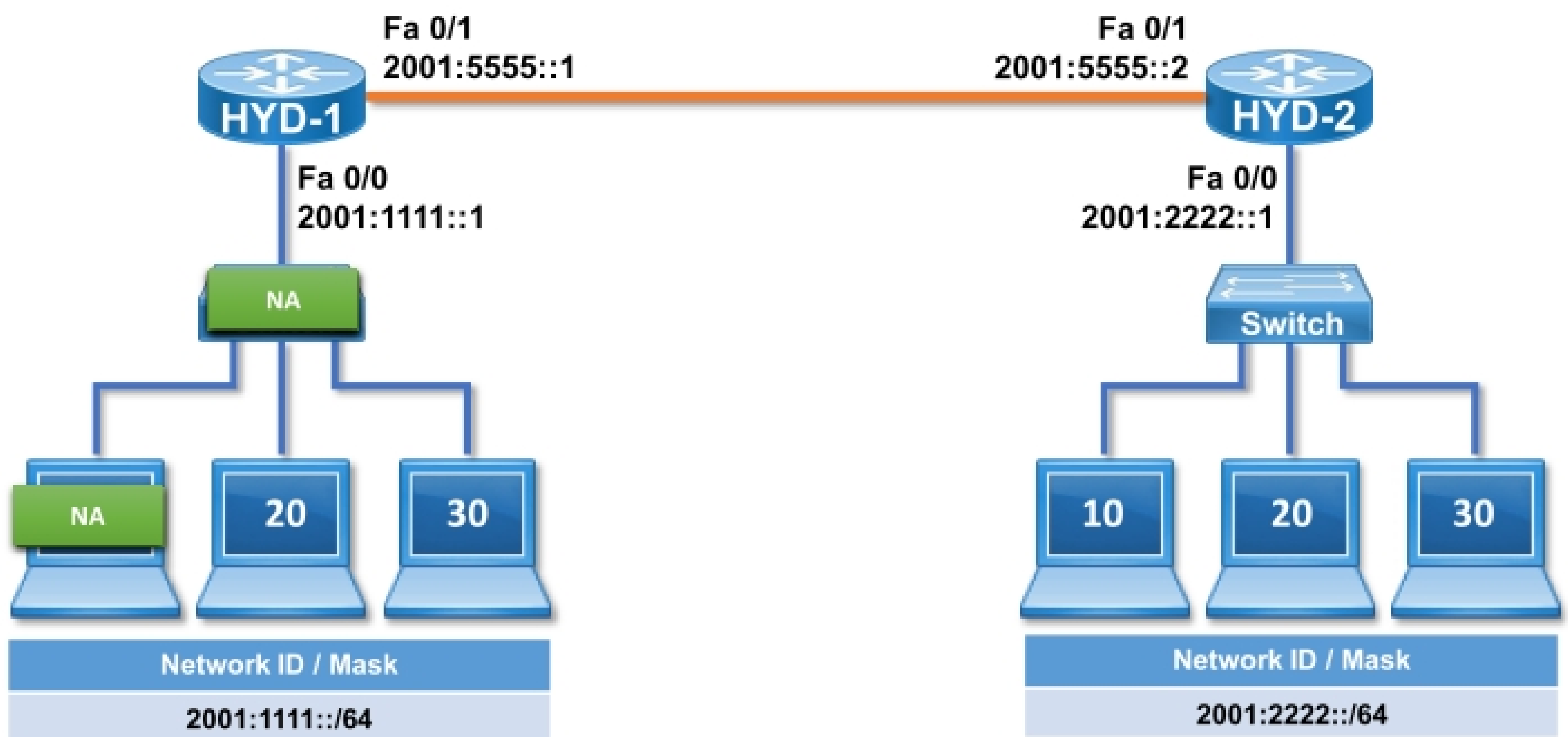
Neighbor Discovery

- IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes.
- Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4 and provides additional functionality.

Neighbor Discovery Message – NS & NA

- Neighbor Solicitation (NS)
  - Message used by Host for requesting Neighbor Host Mac Address
- Neighbor Advertisement (NA)
  - Message used by Neighbor Host for replying Mac Address to requesting Host

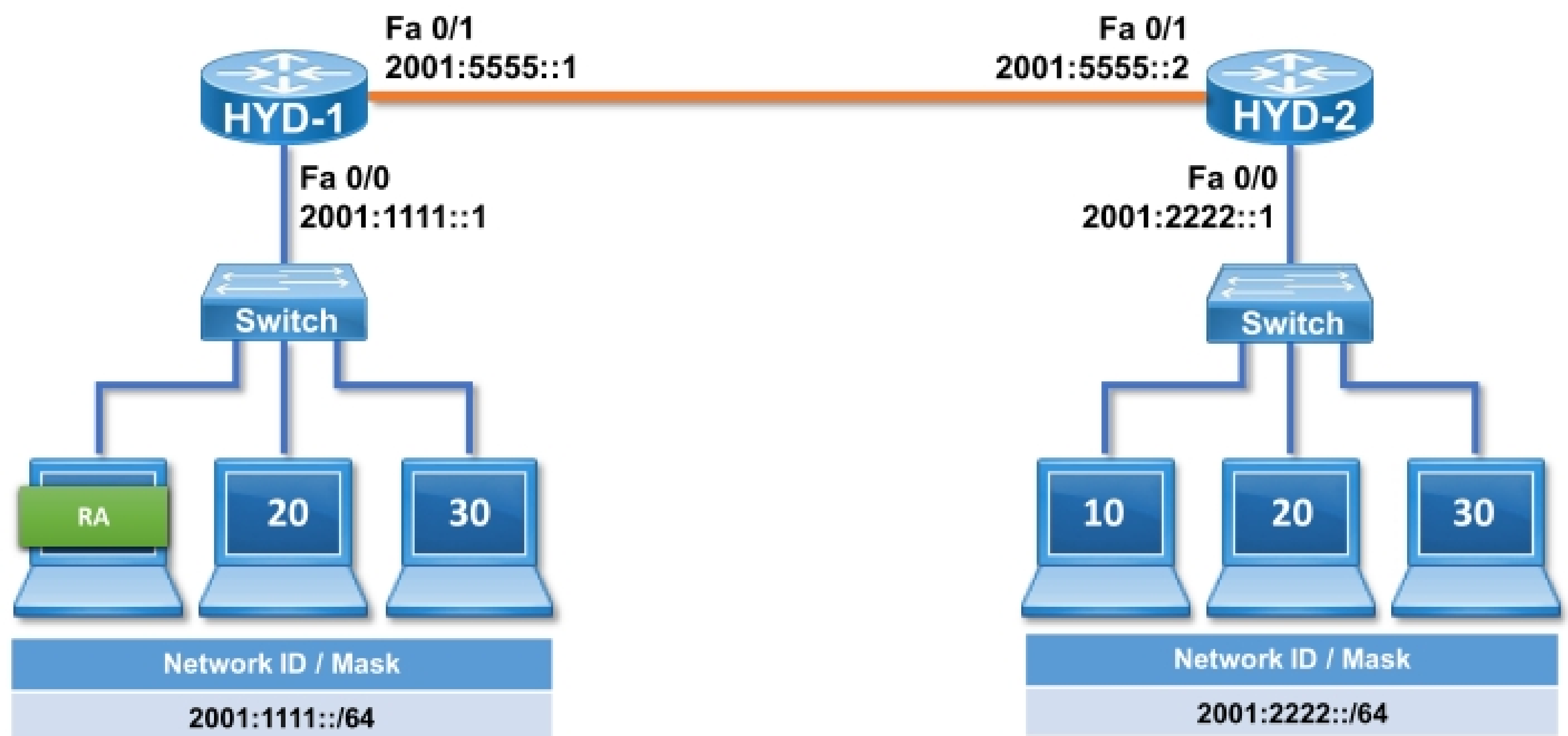
Neighbor Discovery Message – NS & NA



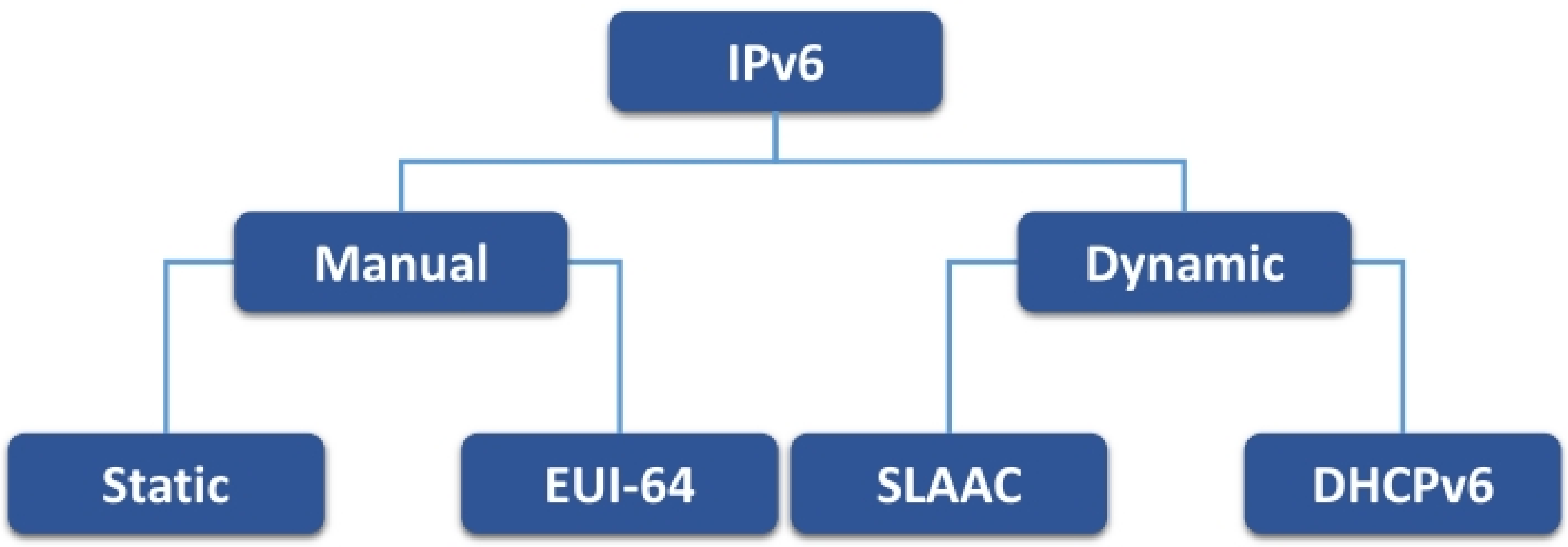
Neighbor Discovery Message – RS, RA & Redirect

- **Router Solicitation (RS)**
  - **Message used by Host for requesting Router IP Address**
- **Router Advertisement (RA)**
  - **Message used by Router for replying to the Host with Router IP Address**
- **Redirect.**
  - **Message used by Host for requesting change of IP Address to Router.**

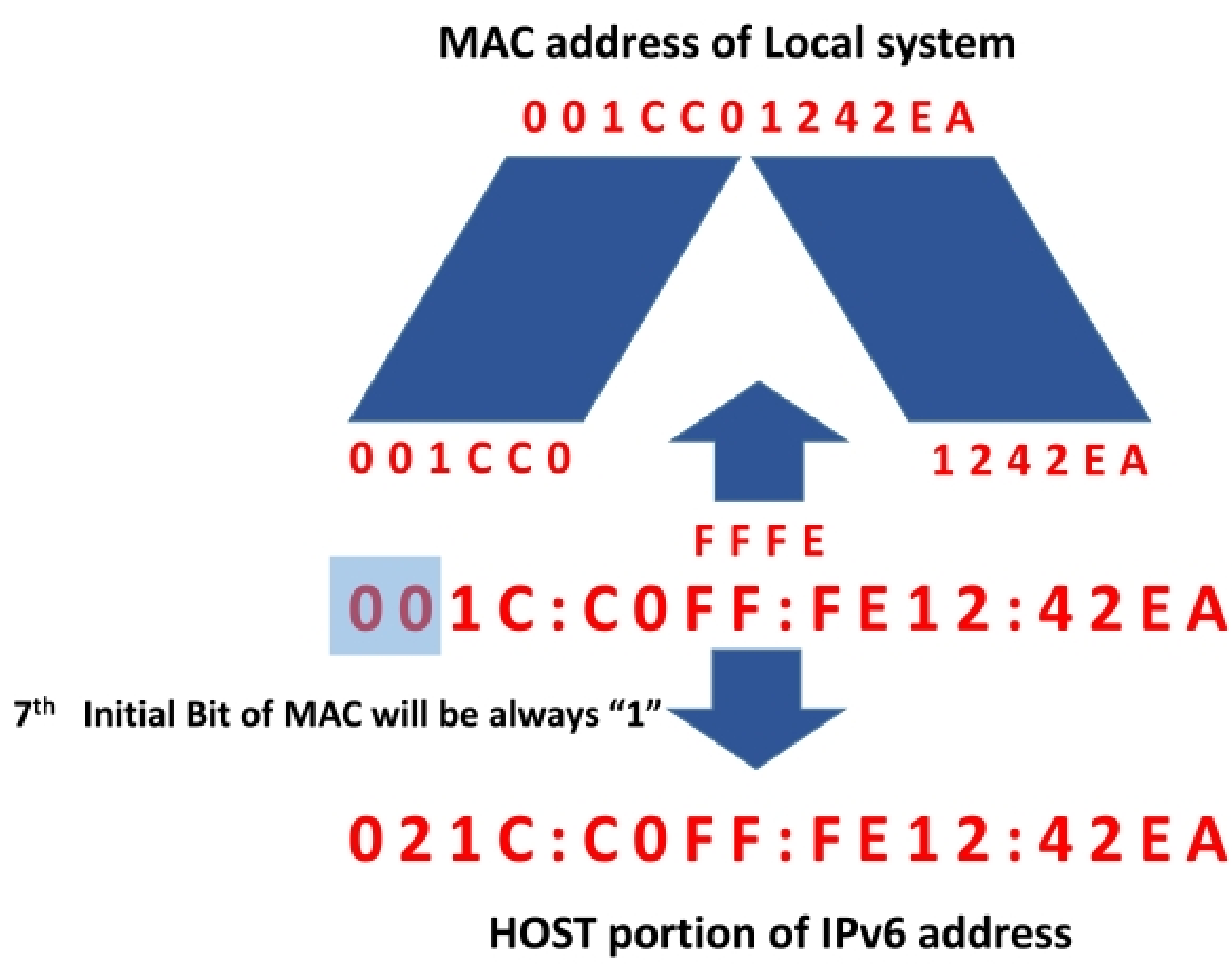
Neighbor Discovery Messages



IPv6 Address Assignment



Host Configuration



IPv6 EUI-64 & SLAAC - Configuration

Assigning IPv6 Address using EUI-64

Router (config) #   ipv6 unicast-routing

Router (config) # interface <interface type> <interface no.>

Router (config-if) # ipv6 enable

Router (config-if) # ipv6 address <IPv6 address> <prefix length> eui-64

Assigning IPv6 Address using SLAAC

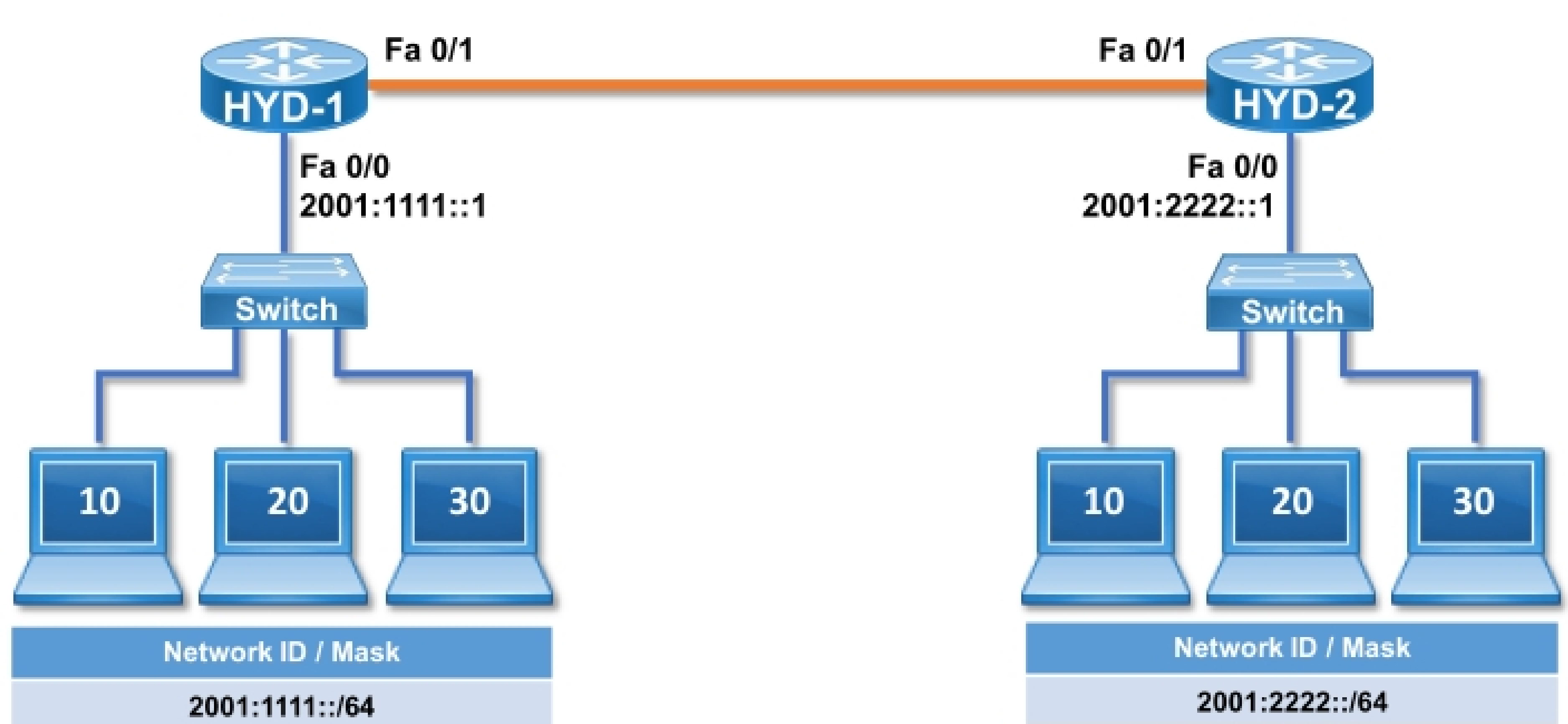
Router (config) #   ipv6 unicast-routing

Router (config) # interface <interface type> <interface no.>

Router (config-if) # ipv6 enable

Router (config-if) # ipv6 address autoconfig

IPv6 EUI-64 & SLAAC - Configuration



IPv6 EUI-64 & SLAAC - Configuration

HYD-1

```
HYD-1 (config) #  ipv6 unicast-routing
HYD-1 (config) #  interface FastEthernet 0/0
HYD-1 (config-if) #  ipv6 enable
HYD-1 (config-if) #  ipv6 address 2001:5555::/64 eui-64
```

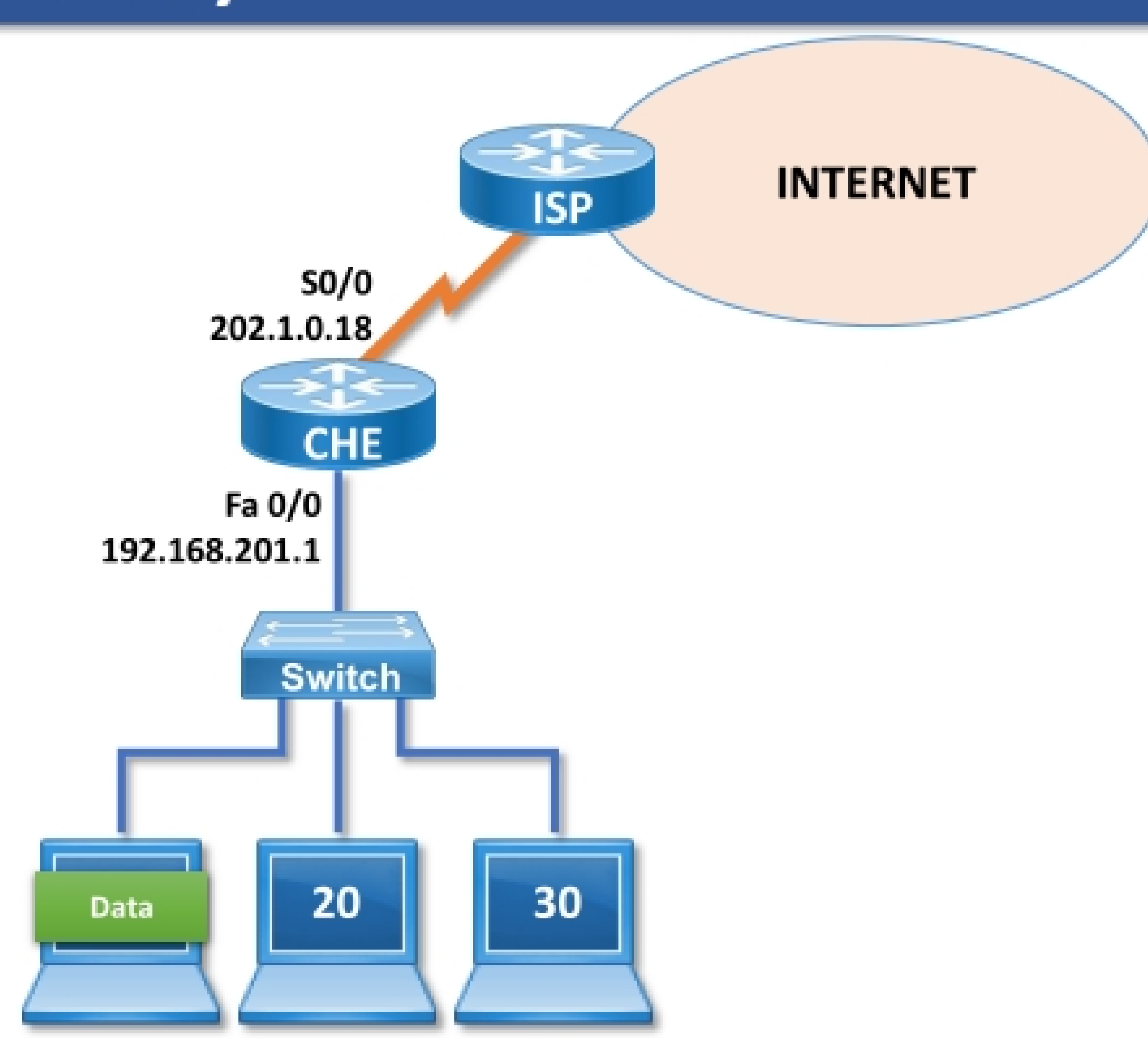
HYD-2

```
HYD-2 (config) #  ipv6 unicast-routing
HYD-2 (config) #  interface fastEthernet 0/0
HYD-2 (config-if) #  ipv6 enable
HYD-2 (config-if) #  ipv6 address autoconfig
```

IPv6 EUI-64 & SLAAC - Verification

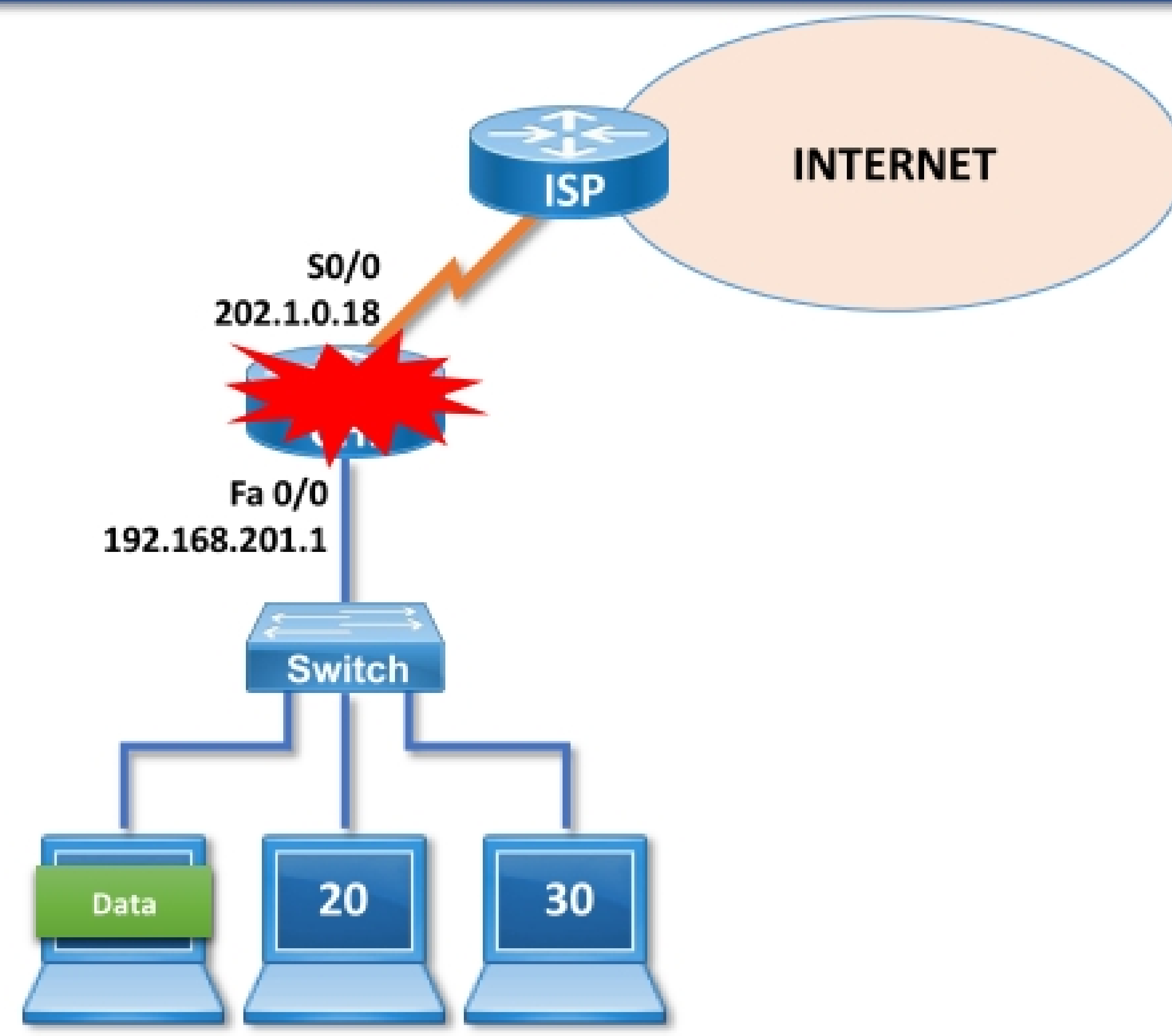
```
Router #  show interface <interface type > <interface no. >
```

Importance of Redundancy



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

Single point of Failure



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

First Hop Redundancy Protocol (FHRP)

- **First Hop Redundancy Protocols (FHRP) are a group of protocols that provide Default Gateway Redundancy if there is more than one path to the same Destination.**
- **The following are FHRP:**
  - **HSRP (Cisco Proprietary)**
  - **VRRP (IETF Standard)**
  - **GLBP (Cisco Proprietary)**

Hot Standby Router Protocol (HSRP)

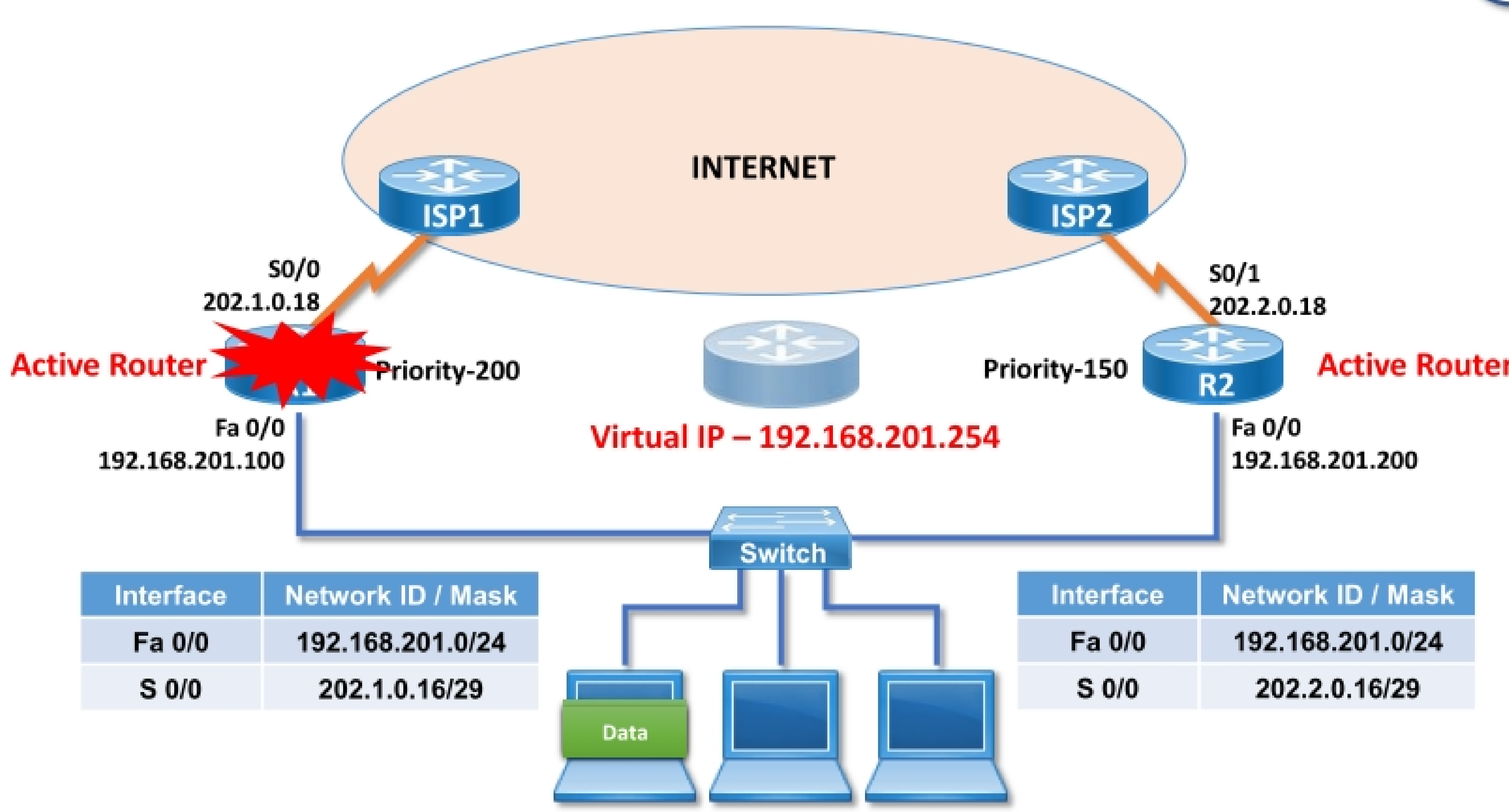
ZOOM TECHNOLOGIES

- HSRP is a Cisco proprietary protocol.
- HSRP groups multiple physical routers
  - i.e. Active router and Standby router into a single virtual router.
- Virtual IP and Mac-addresses are shared between these two physical routers.
- Routers which are grouped together must be assigned the same group number, which can range from 0 to 255
- So when a router goes down or the link into the router fails, there is a second physical device ready to respond to the same default gateway address information

CCIE CCNP CCNA

How HSRP works ?

ZOOM TECHNOLOGIES



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.2.0.16/29

Default Gateway
192.168.201.254

CCIE CCNP CCNA

HSRP Elections

- Uses multicast messages to communicate priority with other routers.
- Default priority is 100.
- Router with the highest priority will be the Active Router and second highest will be the Standby Router
- If the priorities are the same, the first router up becomes the primary.
- The default hold timer is 10 seconds and hello timer is 3 seconds.
- Hello Messages uses multicast address 224.0.0.2 for version 1 using UDP port 1985.

HSRP Terminology

- Active router:
  - Actively forwards the user traffic.
  - Sends the reply for ARP messages requested for virtual mac address.
  - Knows the Virtual Router IP Address.
  - Sends hello messages.

- Standby router:
  - Backup for active router.
  - Sends hello messages.
  - Whenever hello is not received, it takes the role of active router and forwards user traffic.

HSRP Version

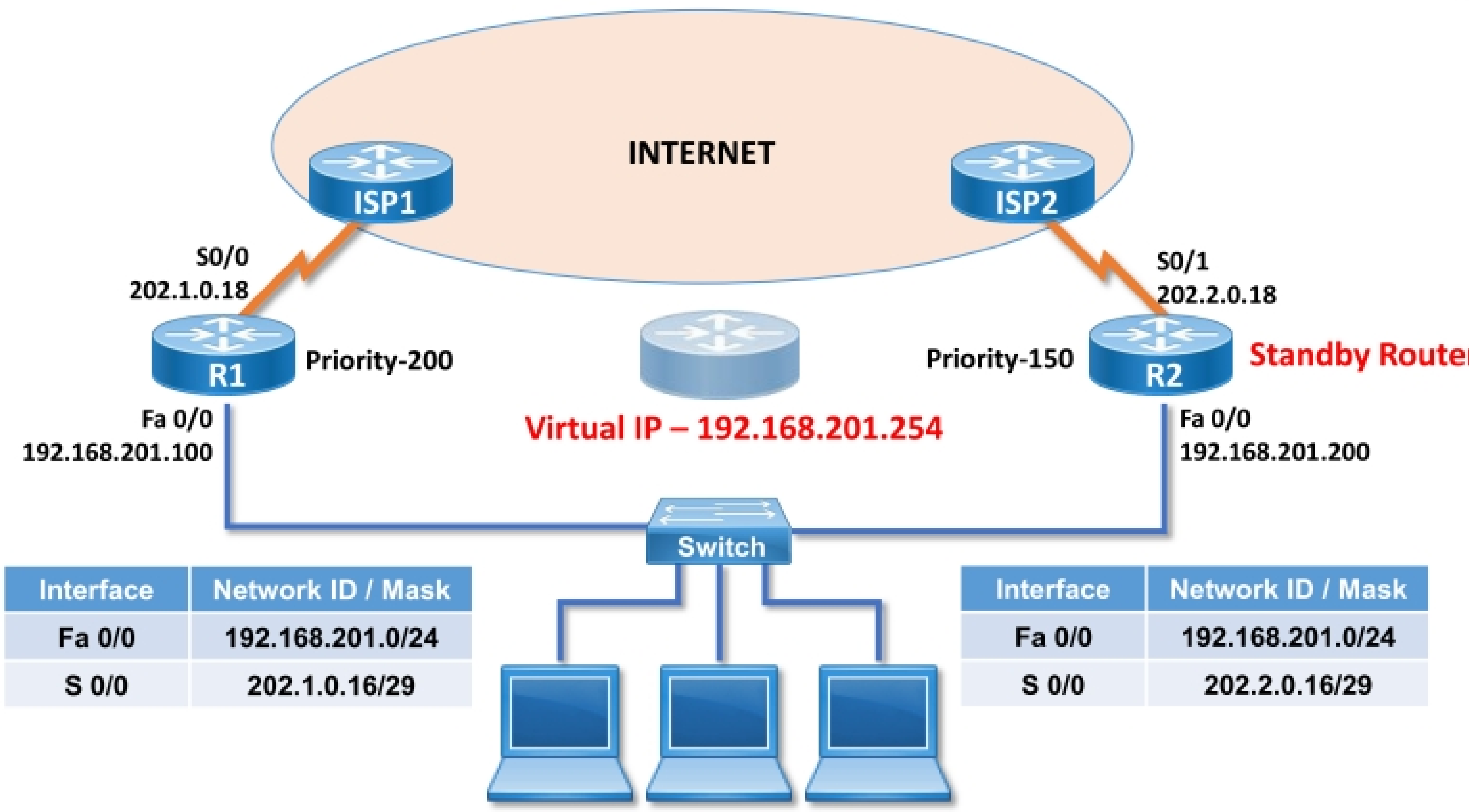
HSRP Version 1	HSRP Version 2
• Hello Messages uses multicast address 224.0.0.2 • Group number range from 0 to 255	• Hello Messages uses multicast address 224.0.0.102 • Group number range from 0 to 4095

HSRP - Configuration

Router (config) # interface < interface type > < no. >
Router (config-if) # standby < hsrp group no. > ip < virtual ip address>
Router (config-if) # standby < hsrp group no. > priority <priority>
Router (config-if) # standby < hsrp group no. > preempt
Router (config-if) # standby version { 1 | 2 }

HSRP - Configuration

ZOOM TECHNOLOGIES



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.2.0.16/29

Default Gateway
192.168.201.254

HSRP - Configuration

ZOOM TECHNOLOGIES

R1

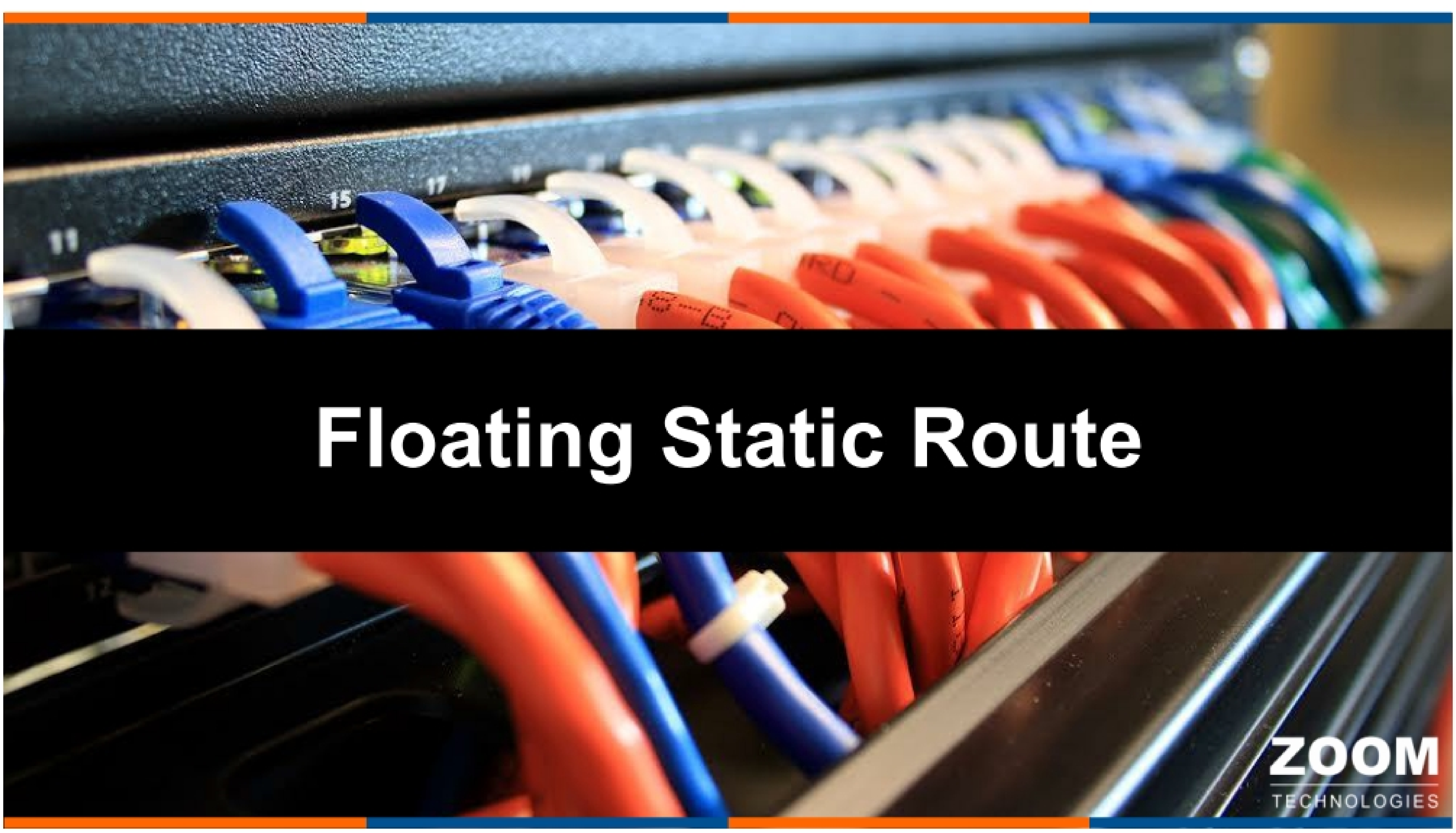
```
R1 (config) # interface fastEthernet 0/0
R1 (config-if) # standby 10 ip 192.168.201.254
R1 (config-if) # standby 10 priority 200
R1 (config-if) # standby 10 preempt
R1 (config-if) # standby version 2
```

R2

```
R2 (config) # interface fastEthernet 0/0
R2 (config-if) # standby 10 ip 192.168.201.254
R2 (config-if) # standby 10 priority 150
R2 (config-if) # standby version 2
```

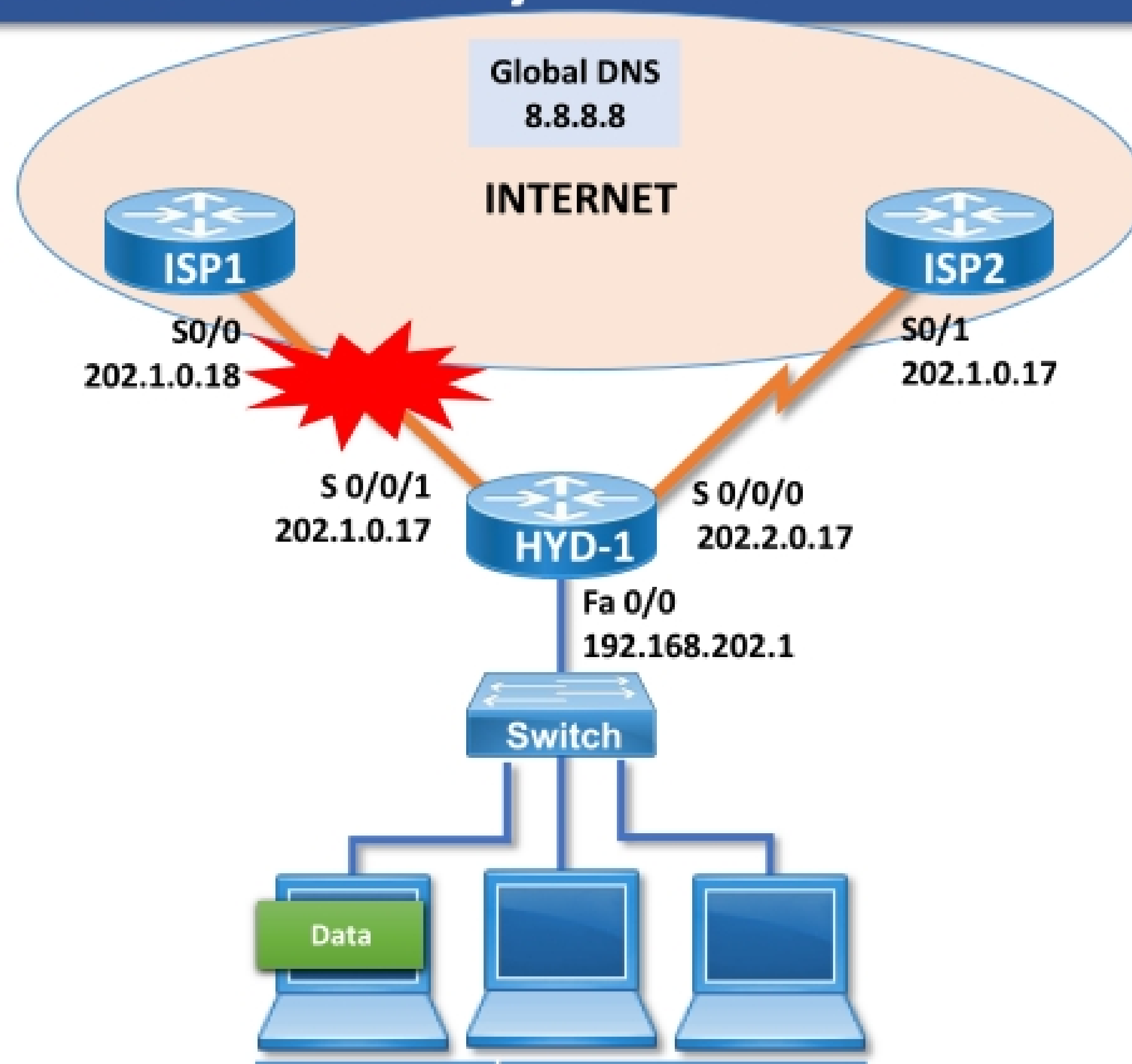
HSRP – Verification

Router # show standby



Importance of WAN Redundancy

ZOOM TECHNOLOGIES



Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	202.1.0.16/29
S 0/0/1	202.2.0.16/29

CCIE CCNP CCNA

Floating Static Route

ZOOM TECHNOLOGIES

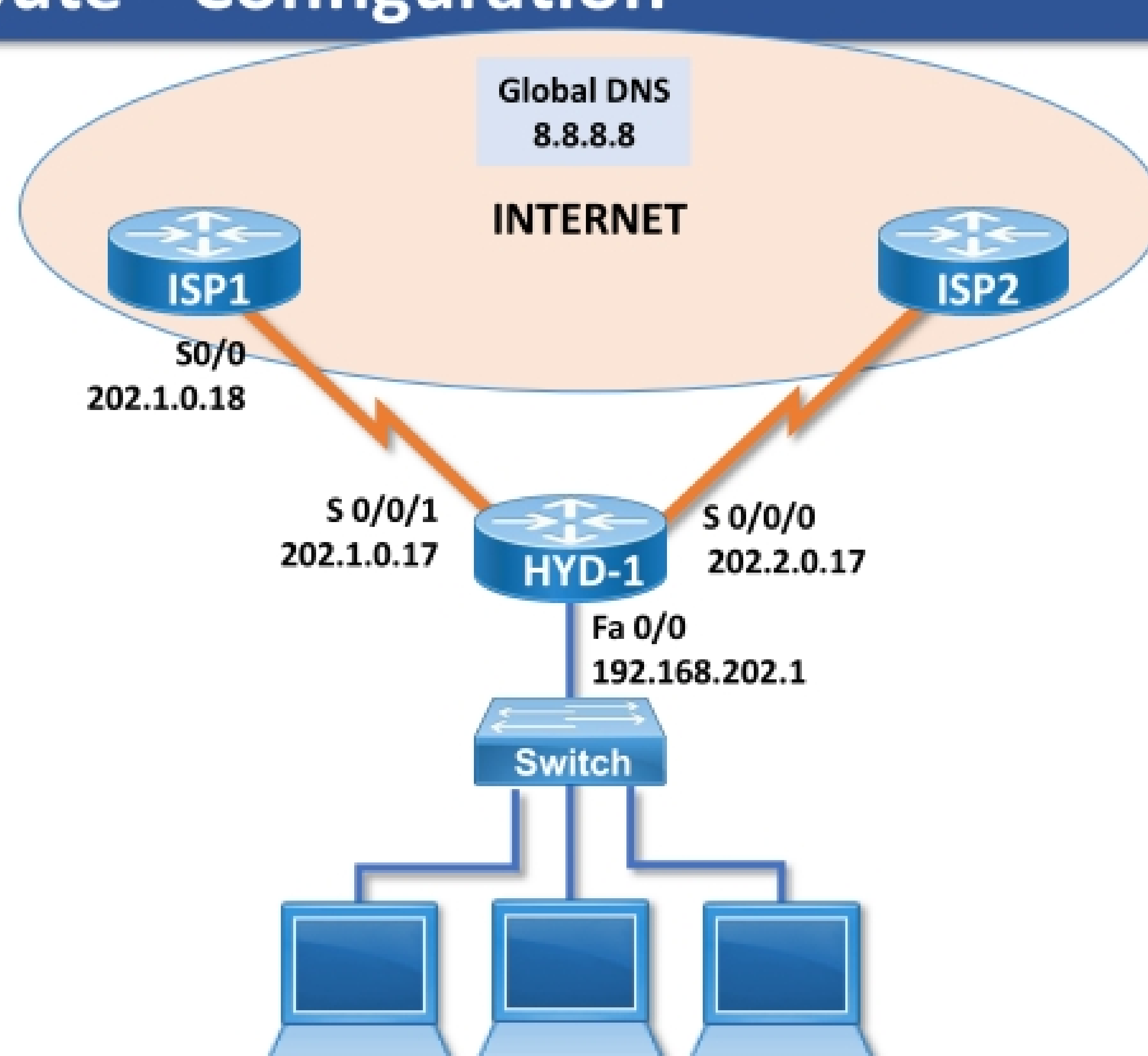
- Floating static routes are static routes configured to provide a backup path in event of a link failure of primary static or dynamic routes.
- The floating static route is only used when the primary route is not available.
- Floating static route is configured with a higher administrative distance than the primary route.

CCIE CCNP CCNA

Floating Static Route - Configuration

Router (config) # ip route < Destination Network ID >
< Destination Subnet Mask > < Exit Interface Type >
< Exit Interface No. > < Administrative Distance >

Floating Static Route - Configuration



Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	202.1.0.16/29
S 0/0/1	202.2.0.16/29

Floating Static Route - Configuration

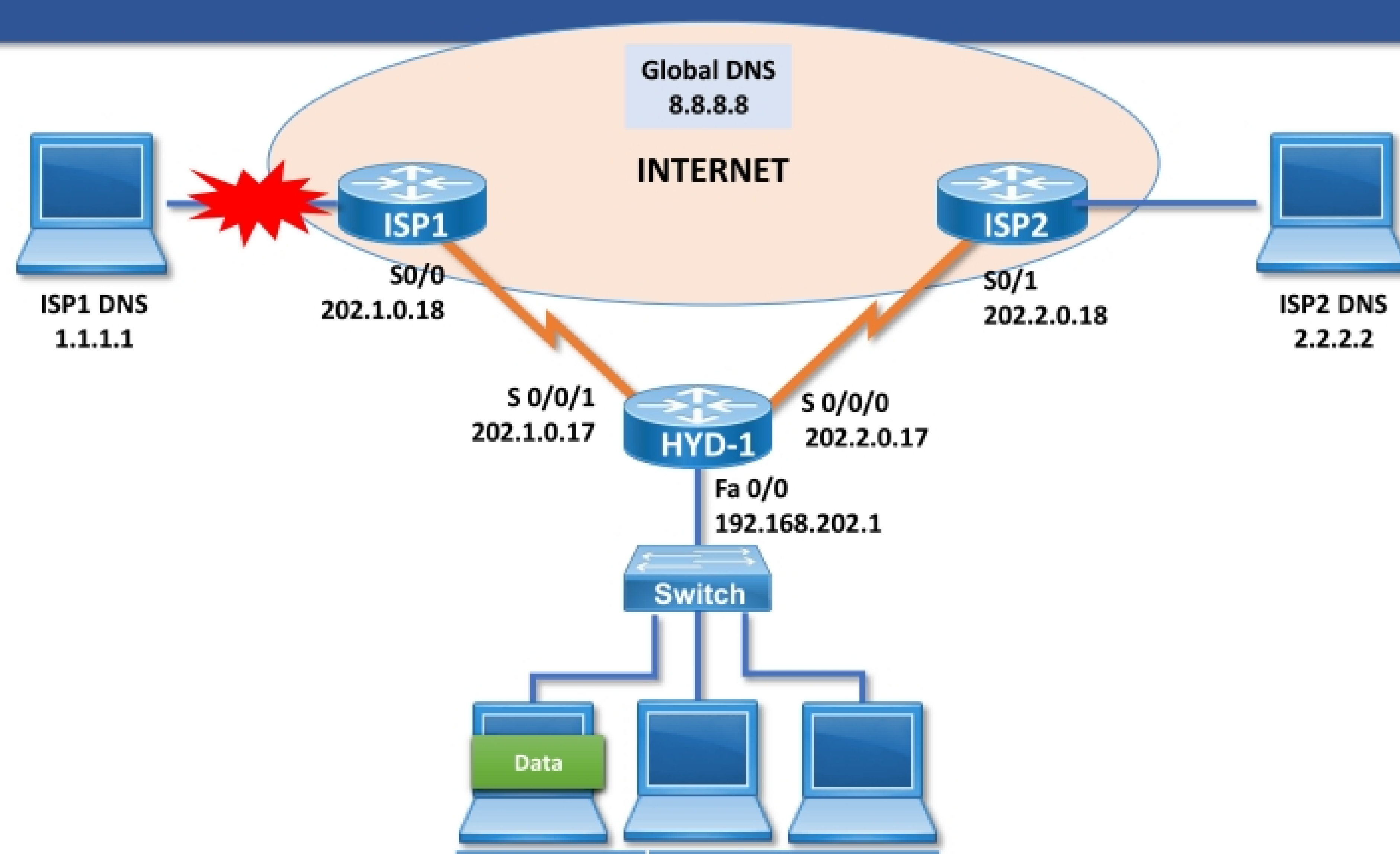
HYD-1 (config) # ip route 0.0.0.0 0.0.0.0 Serial 0/0/1

HYD-1 (config) # ip route 0.0.0.0 0.0.0.0 Serial 0/0/0 2

Floating Static Route - Verification

Router # show ip route

IP SLA



Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	202.1.0.16/29
S 0/0/1	202.2.0.16/29

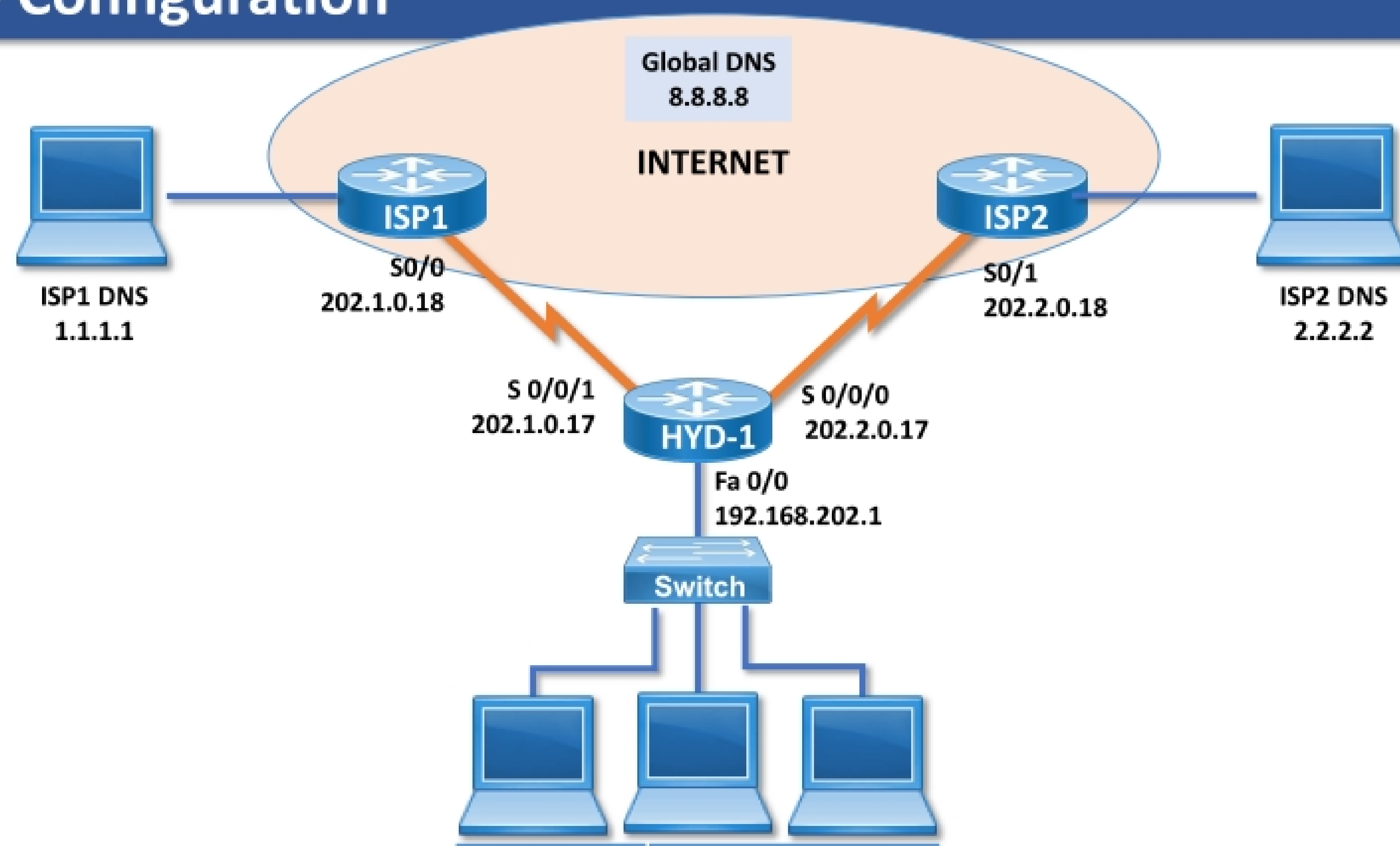
IP SLA

- IP SLAs is a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services.
- IP SLA's uses active traffic-monitoring technology to monitor continuous traffic on the network. This is a reliable method in measuring over head network performance.
- The best and simplest way to achieve WAN redundancy on Cisco devices is to use Reliable Static backup routes with IP SLA tracking.

IP SLA - Configuration

```
Router  (config) # ip sla <operation-number>
Router (config-ip-sla) # icmp-echo <destination ip address>
Router (config-ip-sla-echo) # frequency  < seconds >
Router (config-ip-sla-echo) # exit

Router (config) # ip sla schedule <operation-number> start-time now life forever
Router (config) # track < object-number > ip sla <operation-number>
Router (config-track) # delay down <seconds> up <seconds>
Router (config-track) # exit
Router (config) #  ip route <destination network> <destination subnet mask>
                   <next hop ip address> track < object-number >
```

IP SLA - Configuration



Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24
S 0/0/0	202.1.0.16/29
S 0/0/1	202.2.0.16/29

IP SLA - Configuration

HYD-1

```
HYD-1 (config) # ip sla 1
HYD-1 (config-ip-sla) # icmp-echo 1.1.1.1
HYD-1 (config-ip-sla-echo) # frequency 5
HYD-1 (config-ip-sla-echo) # exit

HYD-1 (config) # ip sla schedule 1 start-time now life forever
HYD-1 (config) # track 10 ip sla 1
HYD-1 (config-track) # delay down 20 up 10
HYD-1 (config-track) # exit
HYD-1 (config) # ip route 0.0.0.0 0.0.0.0 202.1.0.18 track 10
HYD-1 (config) # end
HYD-1 #
```

IP SLA - Verification

Router # show ip route

Local Database Authentication

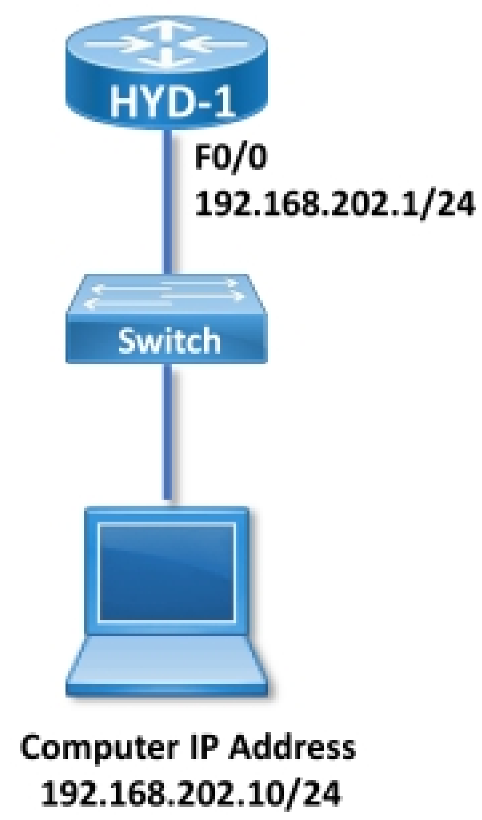
- Usernames and Passwords are created on the device.
- It provides better security than a simple password.
- It is a cost effective and easily implemented security solution.

Local Database Authentication - Configuration

Router (config) # username <user name> password < password >

Router (config) # line vty 0 4
Router (config-line) # login local
Router (config-line) # end
Router (config) #

Local Database Authentication - Configuration

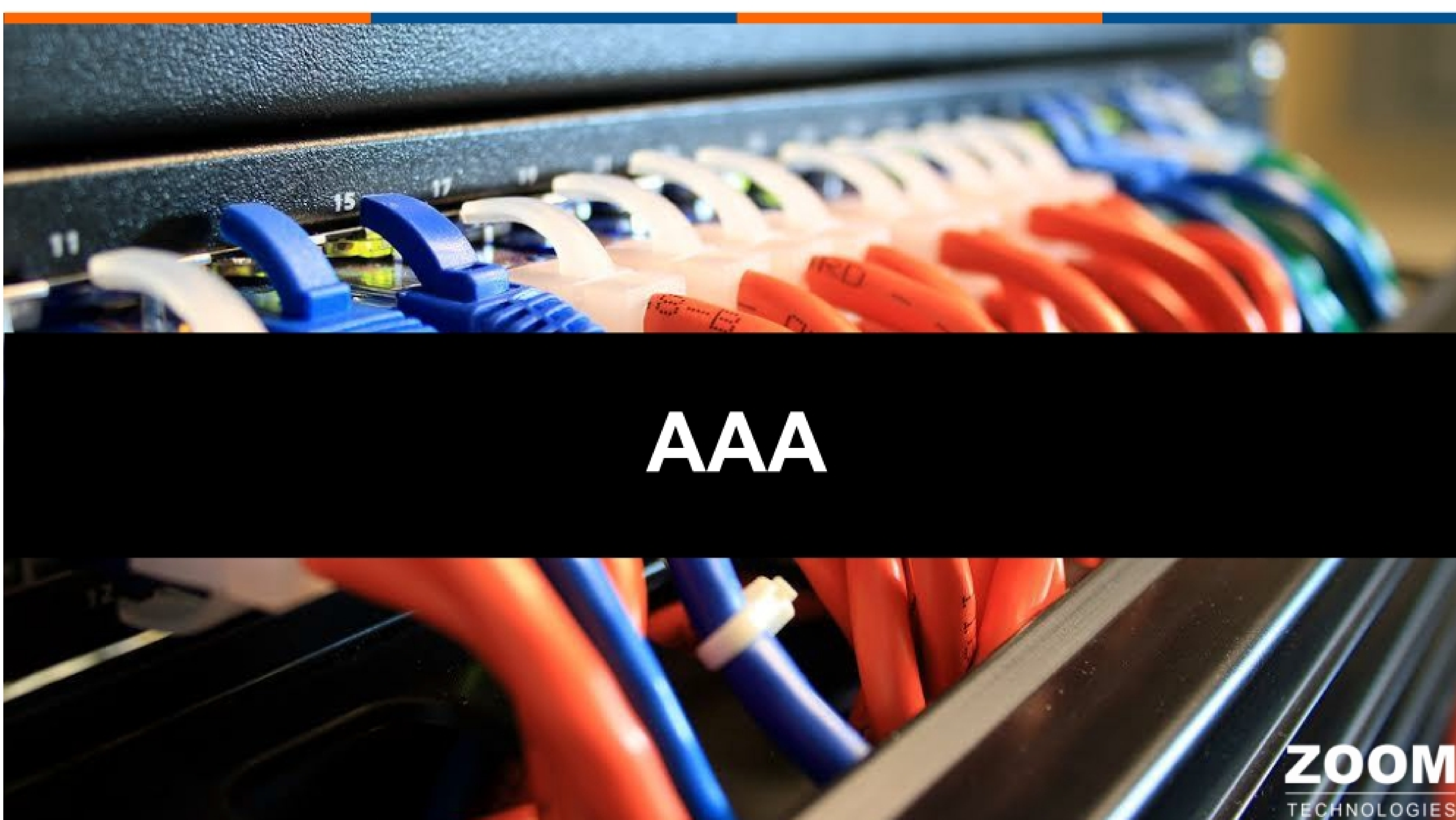


Local Database Authentication - Configuration


```
HYD-1 (config) # username zoom password  cisco
HYD-1 (config) # line vty 0 4
HYD-1 (config-line) # login local
HYD-1 (config-line) # end
```

Disadvantage of Local Database Authentication

- **Local Database needs to be replicated on all network devices**
- **Better and Scalable solution is to use AAA Server.**



AAA

- Authentication
  - Authentication provides the method of identifying users
- Authorization
  - Authorization provides a method of controlling access to what a user can do.
- Accounting
  - Accounting provides a method for collecting and sending security server information used for billing, auditing and reporting.

AAA Advantages

- Increased flexibility and control of access configuration
- Scalability
- Multiple backup systems
- Standardized authentication methods
  - RADIUS, TACACS+ and Kerberos

AAA Protocols

- **Terminal Access Controller Access Control System (TACACS)**
- **Remote Access Dial In User Service (RADIUS)**

TACACS v/s RADIUS

TACACS	RADIUS
• TACACS+ is Cisco proprietary protocol • TACACS+ uses TCP as Transport Layer Protocol • TACACS+ encrypts the entire communication • TACACS+ treats Authentication, Authorization and Accountability differently	• RADIUS is supported by multiple vendors • RADIUS uses UDP as Transport layer Protocol • RADIUS encrypts passwords only • RADIUS combines Authentication and Authorization

AAA Server Based Authentication - Configuration

ZOOM TECHNOLOGIES

Router (config) # aaa new-model>

Router (config) # tacacs-server host < server ip address >

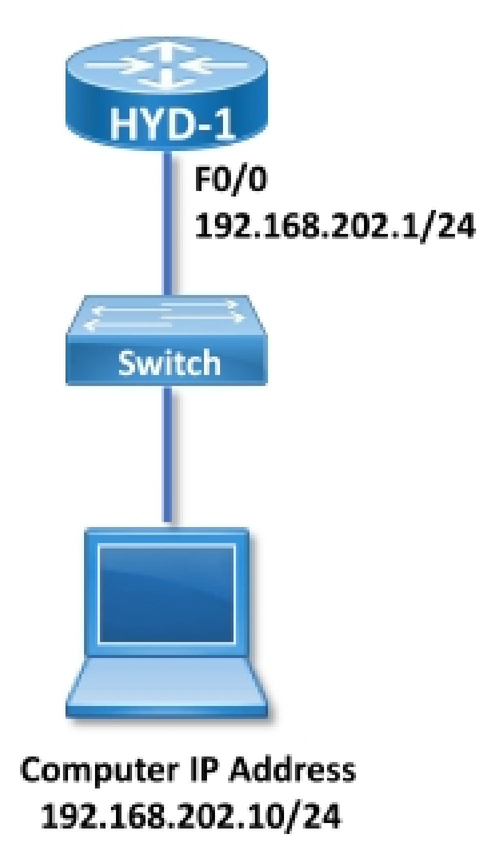
Router (config) # tacacs-server key < secret key >

Router (config) # aaa authentication login default group tacacs local

CCIE CCNP CCNA

AAA Server Based Authentication - Configuration

ZOOM TECHNOLOGIES



CCIE CCNP CCNA

AAA Server Based Authentication - Configuration

HYD-1

```
HYD-1 (config) #  aaa new-model
HYD-1 (config) # tacacs-server host 192.168.202.10
HYD-1 (config) # tacacs-server key cisco
HYD-1 (config) # aaa authentication login default group tacacs local
```

Telnet

- Telnet is used to remote login on the Network devices for configuration.
- It works on TCP Port 23.
- Data is sent in clear text between host and network device, it is not secure communication.

Secure Shell (SSH)

- SSH is used for securely remote login on the Network devices for configuration.
- It works on TCP Port 22.
- It provides data encryption between host and network device.
- Cisco IOS should support encryption for enabling SSH.

SSH - Configuration

Router (config) # ip domain-name < domain name>

Router (config) # crypto key generate rsa

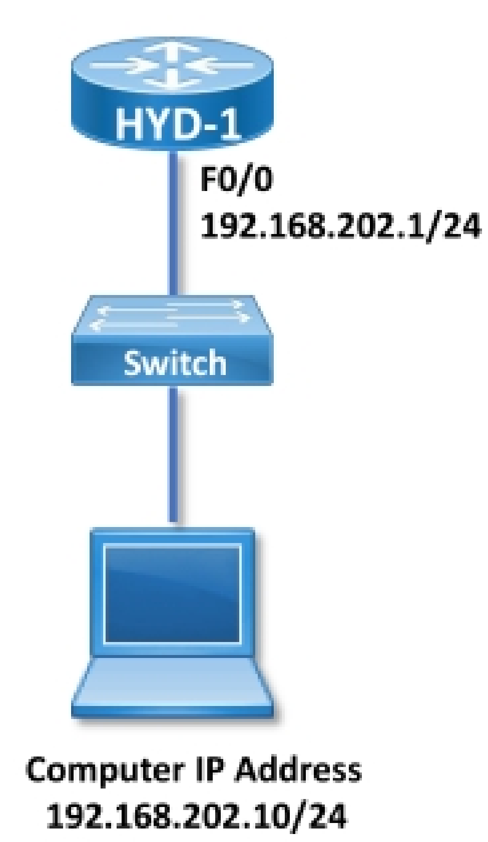
Router (config) # line vty 0 4

Router (config-line) # login local

Router (config-line) # transport input ssh

Router (config-line) # end

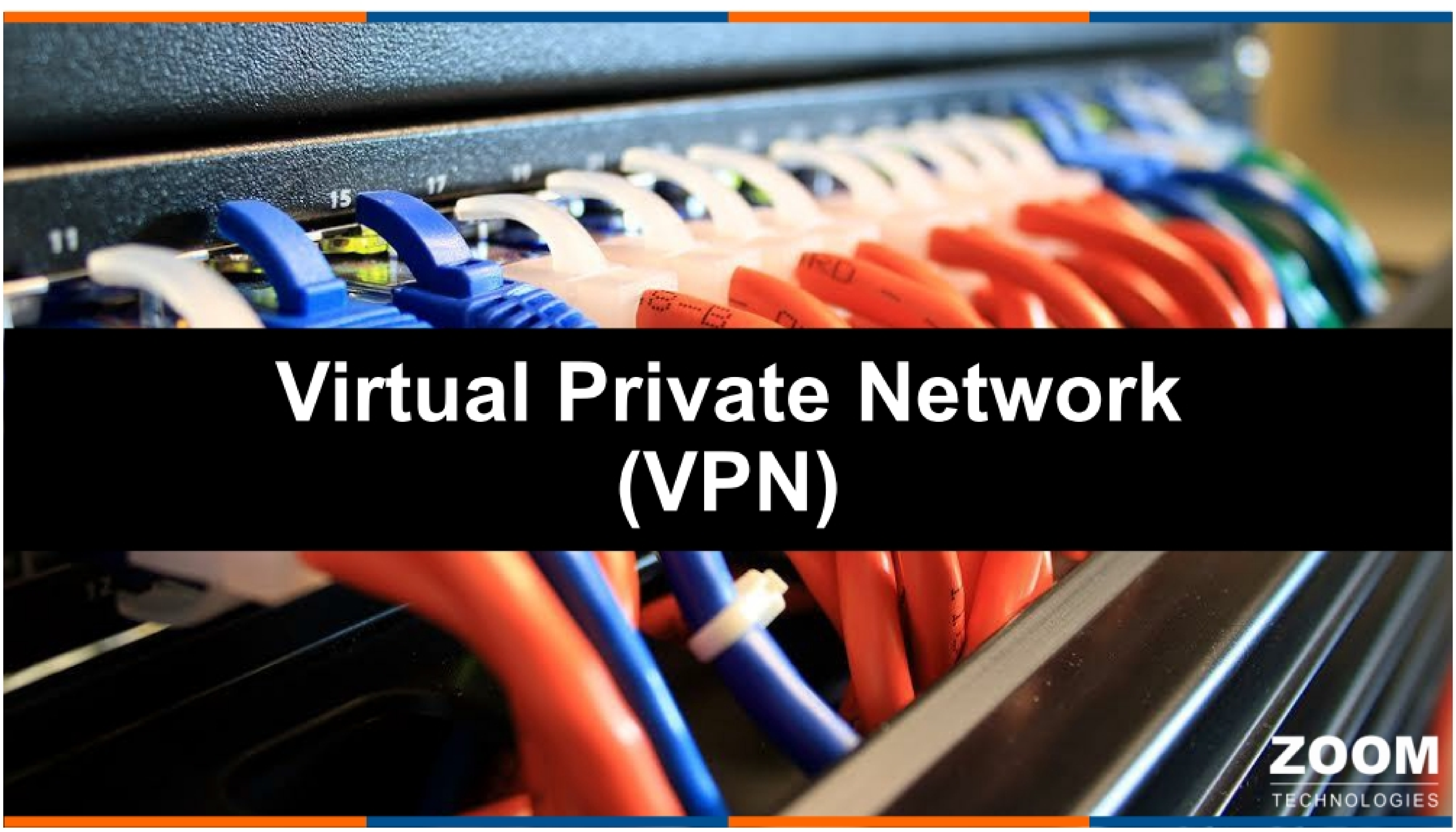
SSH - Configuration



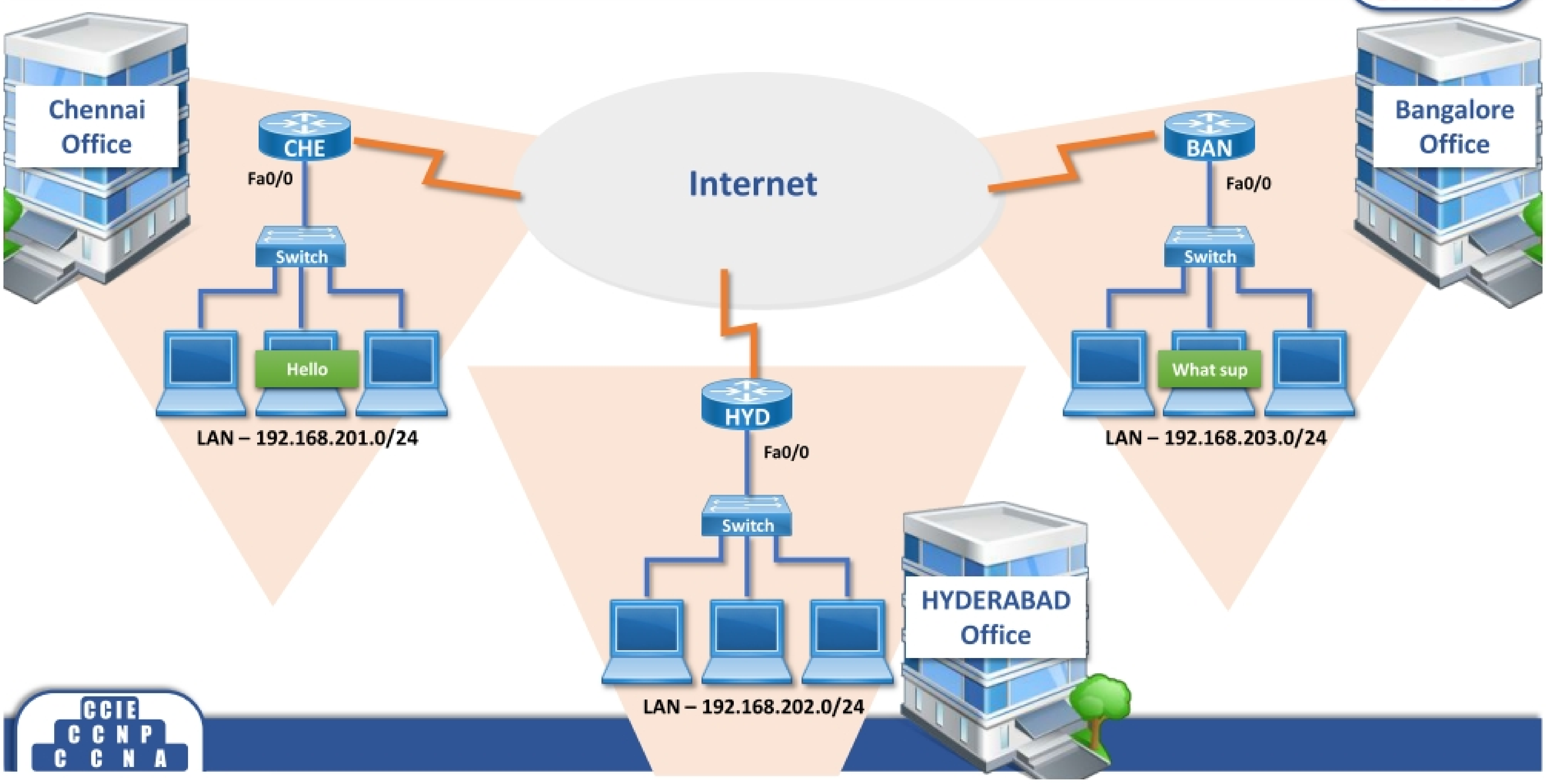
SSH - Configuration

HYD-1

```
HYD-1 (config) # ip domain-name zoom.com
HYD-1 (config) # crypto key generate rsa
 HYD-1 (config) # line vty 0 4
HYD-1 (config-line) # login local
HYD-1 (config-line) # transport input ssh
HYD-1 (config-line) # end
```



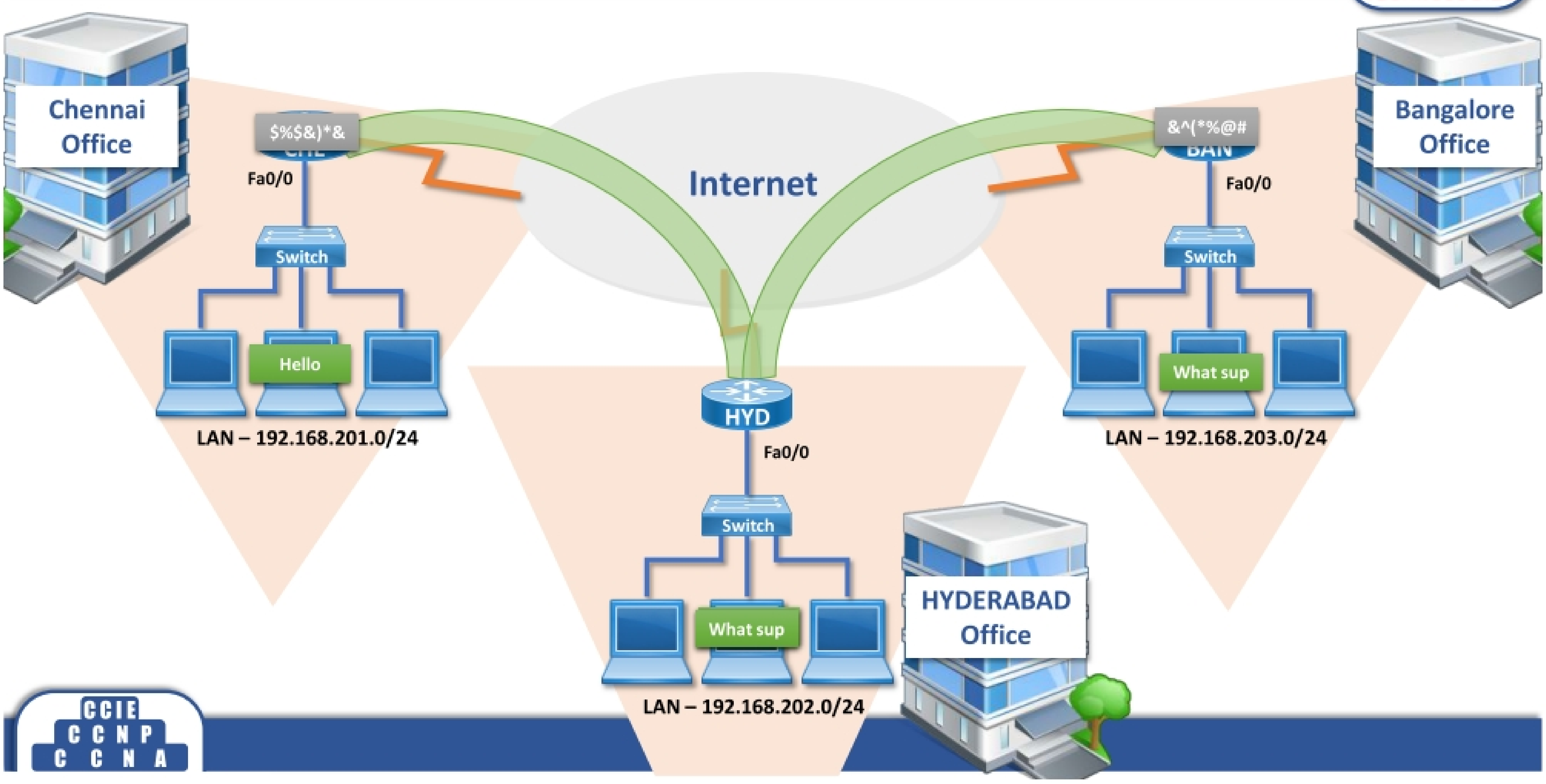
Communication via Internet



Virtual Private Network

- **It provides a private communication channel over a public network.**
- **Provides security**
- **Provides point to point connectivity**
- **Scalability**

VPN



Features of VPN

- Confidentiality (Privacy)
- Authentication
- Data integrity
- Anti-replay

Types of VPN

- GRE
- IPSec VPN
- SSL VPN
- DMVPN (Dynamic Multipoint VPN)

Generic Routing Encapsulation (GRE)

- GRE is a tunneling protocol that was originally developed by Cisco.
- GRE provides tunneling of Non-IP traffic (IPX and Appletalk) and Multicast traffic (which is not done by IPSec).
- However, GRE provides only tunneling without any encryption.

NOTE :

Static Route should be configured towards remote LAN network via tunnel interface

GRE - Configuration

Router (config) # interface tunnel < no. >

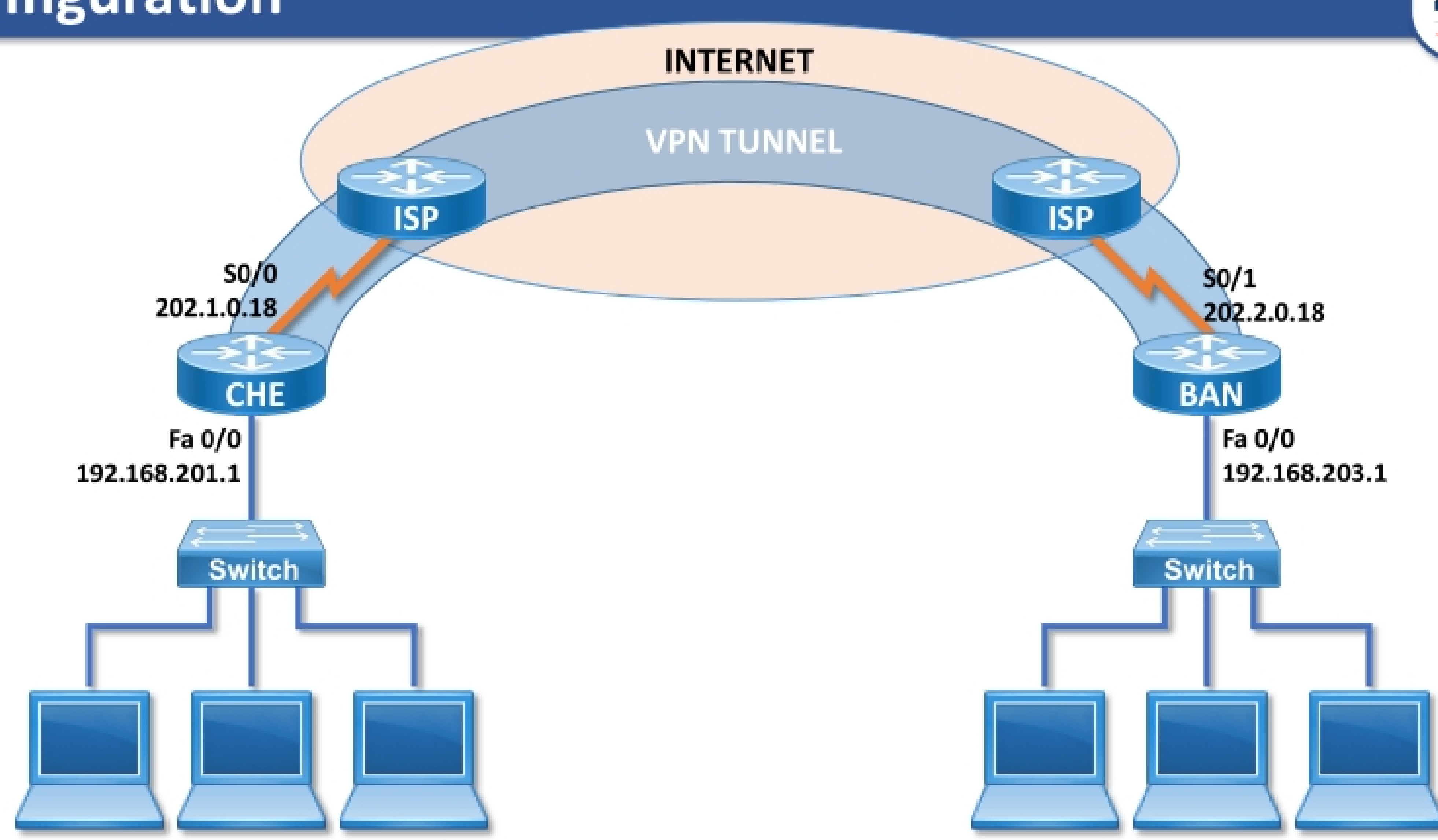
Router (config-if) # ip address < address > < subnet mask >

Router (config-if) # tunnel source < tunnel source ip address >

Router (config-if) # tunnel destination < tunnel destination ip address >

Router (config-if) # end

GRE - Configuration



Interface	Network ID / Mask
Fa 0/0	192.168.201.0/24
S 0/0	202.1.0.16/29

Interface	Network ID / Mask
Fa 0/0	192.168.203.0/24
S 0/0	202.2.0.16/29

GRE - Configuration

CHE

```
CHE (config) # int tunnel 0
CHE (config-if) # ip add 1.1.1.1 255.255.255.0
CHE (config-if) # tunnel mode gre ip
CHE (config-if) # tunnel source serial 0/0
CHE (config-if) # tunnel destination 202.2.0.18
CHE (config-if) # end
```

BAN

```
BAN (config) # int tunnel 0
BAN (config-if)# ip add 1.1.1.2 255.255.255.0
BAN (config-if) # tunnel mode gre ip
BAN (config-if)# tunnel source serial 0/1
BAN (config-if)# tunnel destination 202.1.0.18
BAN (config-if)# end
```

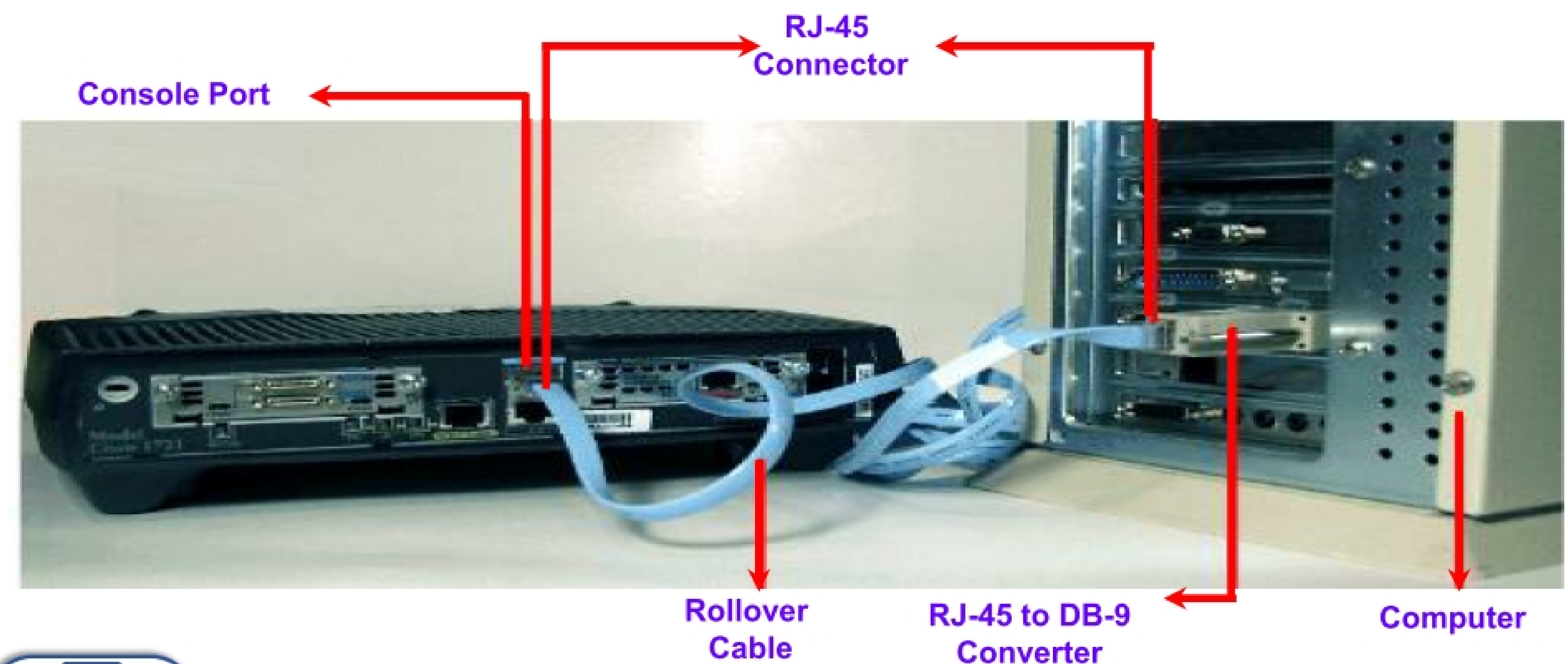
GRE – Verification

```
Router # show interface tunnel  < no.>
```

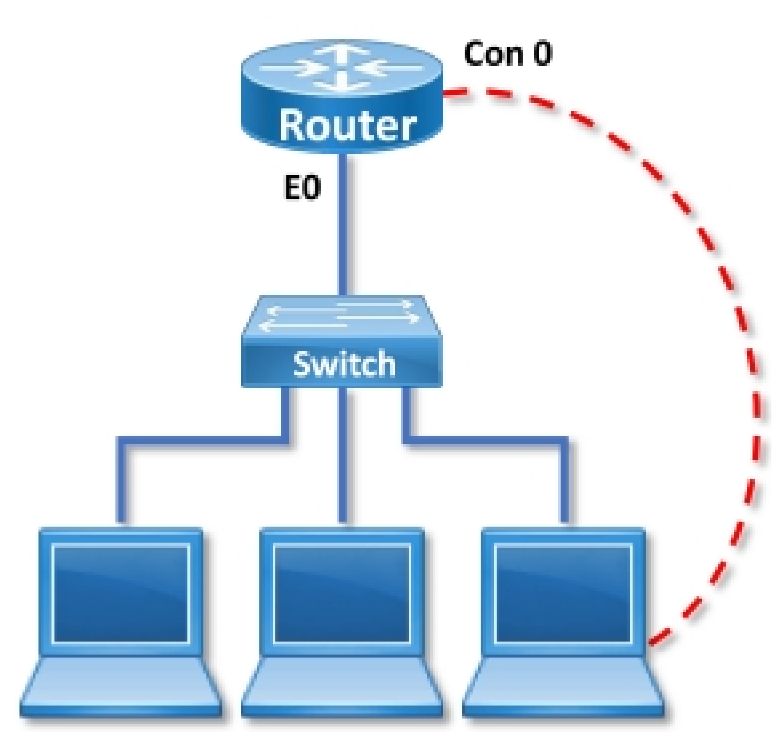
Password Recovery - Steps

- Connect the console cable from Router console Port to PC COM port
- Open the Emulation Software (Putty)
- Restart the Router
- Press Ctrl + Break to Enter into Rommon mode

Console Connectivity



Password Recovery



Password Recovery - BOOT Sequence

Power On Self Test – checks the hardware	POST
ROM loads Bootstrap program and searches for the IOS	ROM
IOS from Flash is loaded	FLASH
Boot process is completed bypassing startup configuration	RAM

Configuration Register - 0x2142

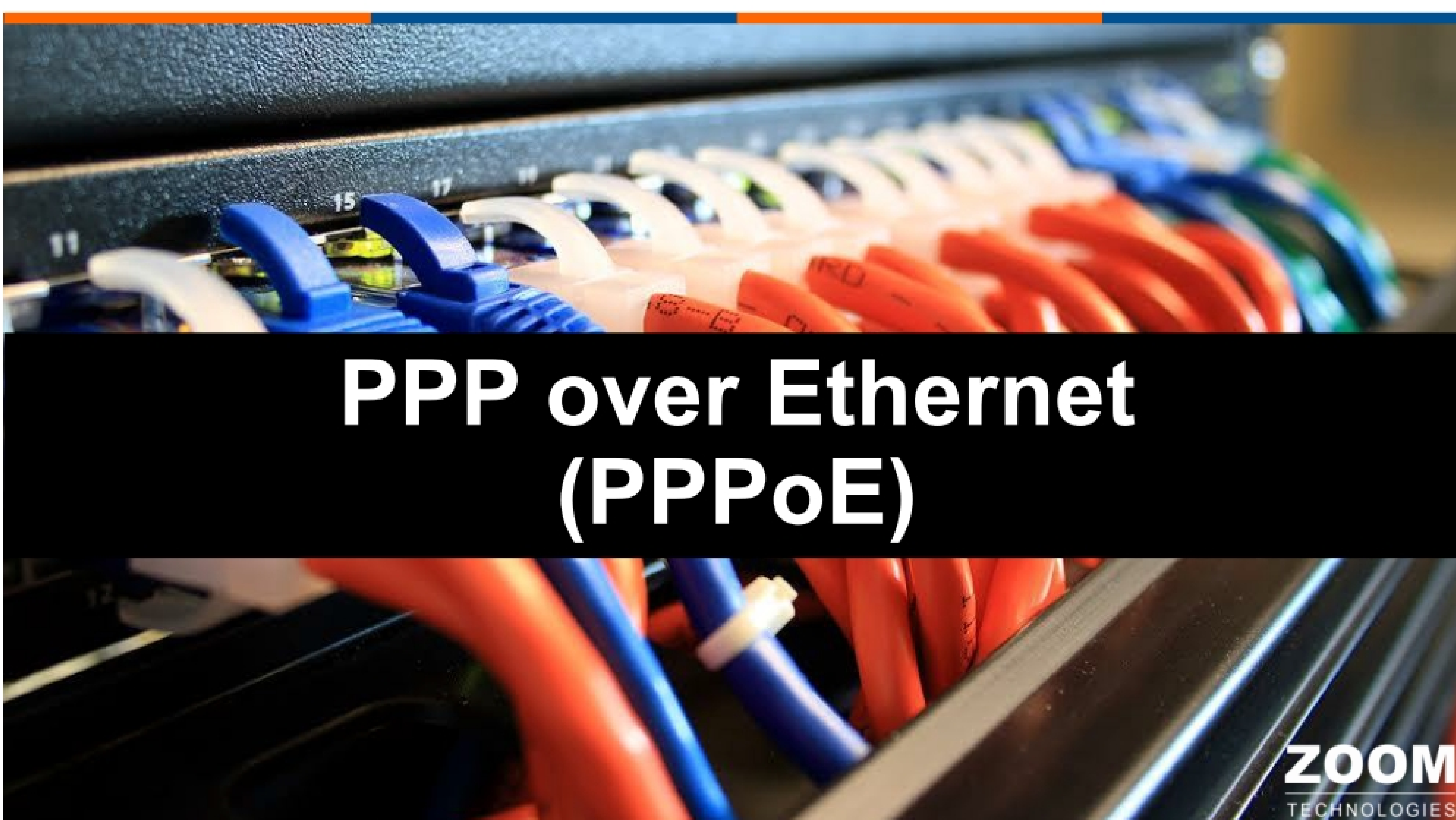
Password Recovery - Steps

Rommon1 > confreg 0x2142

Rommon2 > reset

Password Recovery - Steps

```
Router >  enable
Router #  copy startup-config  running-config
Router #  configure terminal
Router (config) #  enable  secret  < new password >
Router (config) #  interface  FastEthernet 0/0
Router (config-if) #  no shutdown
Router (config) #  exit
Router (config) #  config-register 0x2102
Router (config) #  end
Router #  write
Router #  reload
```



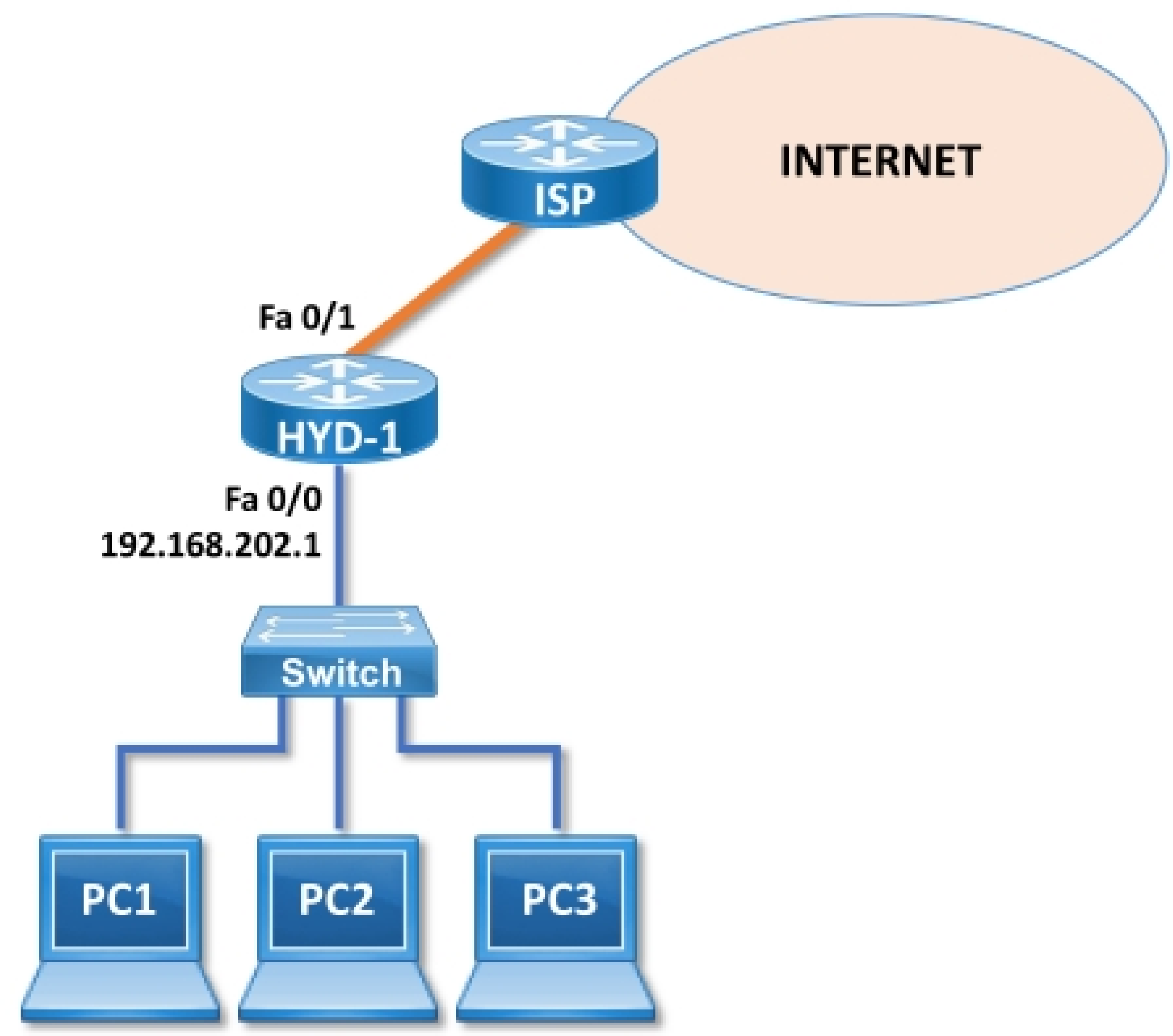
PPP over Ethernet (PPPoE)

- **PPP over Ethernet (PPPoE) is a method of encapsulating PPP frames so that they can be sent over an Ethernet network.**
- **PPPoE is generally used by Internet Service Providers (ISPs) to provide Broadband Internet access based upon user authentication.**
- **We can configure Cisco router as PPPoE Client for Broadband Internet Access.**

PPPoE Client - Configuration

```
Router (config) #  interface  < ethernet interface >  < no. >
Router (config-if) #  no  ip  address
Router (config-if) # pppoe enable
Router (config-if) # pppoe-client dial-pool-number <no.>
Router (config-if) # exit
Router (config) #  interface dialer  < no. >
Router (config-if) # mtu 1492
Router (config-if) # ip address negotiated
Router (config-if) # encapsulation ppp
Router (config-if) # ppp authentication pap callin
Router (config-if) # ppp pap sent-username < username > password < password >
Router (config-if) # dialer pool < no. >
Router (config-if) # ppp ipcp route default
Router (config-if) # end
```

PPPoE Client - Configuration



Interface	Network ID / Mask
Fa 0/0	192.168.202.0/24

PPPoE Client - Configuration

HYD-1

```
HYD-1 (config) # interface fastethernet 0/1
HYD-1 (config-if) # no ip address
HYD-1 (config-if) # pppoe enable
HYD-1 (config-if) # pppoe-client dial-pool-number 1
HYD-1 (config-if) # exit
HYD-1 (config) # interface dialer 1
HYD-1 (config-if) # mtu 1492
HYD-1 (config-if) # ip address negotiated
HYD-1 (config-if) # encapsulation ppp
HYD-1 (config-if) # ppp authentication pap callin
HYD-1 (config-if) # ppp pap sent-username cisco password ccna
HYD-1 (config-if) # dialer pool 1
HYD-1 (config-if) # ppp ipcp route default
HYD-1 (config-if) # end
```

PPPoE Client – Verification

Router # show interfaces dialer <no. >

Binary 8	4	2	1	Decimal	Hexa-decimal
0	0	0	0	0	0
0	0	0	1	1	1
0	0	1	0	2	2
0	0	1	1	3	3
0	1	0	0	4	4
0	1	0	1	5	5
0	1	1	0	6	6
0	1	1	1	7	7
1	0	0	0	8	8

Binary 8	4	2	1	Decimal	Hexa-decimal
1	0	0	1	9	9
1	0	1	0	10	A
1	0	1	1	11	B
1	1	0	0	12	C
1	1	0	1	13	D
1	1	1	0	14	E
1	1	1	1	15	F

MCSE-2012 Full Course

MICROSOFT CERTIFIED SOLUTIONS EXPERT

Practicals in real-time environment. Detailed curriculum with all 5 papers

Duration: 1 Month | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

CCNA (v 2.0) Full Course

CISCO CERTIFIED NETWORK ASSOCIATE

Cisco Routers with BSNL/TELCO MUX & Live Channelised E1

Duration: 1 Month | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

LINUX ADMINISTRATION

COMPLETE RHCE LINUX

Practicals on Live Web Administration + Integration of Windows with Linux/Unix (Samba Server)

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.00 • Afternoon: 1.30 • Evening: 7.00

PC HARDWARE & NETWORKING

WORKSHOP ON EMERGING TECHNOLOGIES

- Ethical Hacking, Cyber Security and Firewall
- VMware vSphere and MS Private Cloude
- Open Source: A glimpse into advance Linux
- Cisco WAN Technology & Collaboration

Free MCSE & CCNA Exam Practice Questions

Complete Package for Only

Fees: ₹ 5,900/-

+ 15% Service Tax

Duration: 3 Months

4 Hrs Per Day

100% GUARANTEED JOB ASSISTANCE

EHCE | Ethical Hacking & Countermeasures Expert

Course is mapped to EHCE course from US-Council (www.us-council.com)

(Pre requisite is CCNA / MCSE / LINUX)

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹ 9,500/-
+ 15% Service Tax

CCNP R&S

CISCO CERTIFIED NETWORK PROFESSIONAL

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 • Afternoon: 2.00 • Evening: 6.00

- Labs on latest routers with IOS version 15.X

Monitoring, Diagnostics & Troubleshooting Tools

- PRTG
- Wireshark
- SolarWinds, etc.

Exam Practice Challenge Labs

Fees: ₹ ~~10,000/-~~

Introductory Special Offer

Fees: ₹ 5,500/-

+ 15% Service Tax

CCIE R&S

CISCO CERTIFIED INTERNETWORK EXPERT

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 • Evening: 6.00

- Individual Rack For Every Student
- Real time scenarios by 20+ years experienced CCIE certified industry expert who has worked on critical projects worldwide.

Written + Lab Exam Focus

FREE Full Scale 8 Hours Exam Lab Included

Unlimited Lab Access For 1 Year

Fees: ₹ ~~25,000/-~~

Introductory Special Offer

Fees: ₹ 9,999/-

+ 15% Service Tax

MICROSOFT EXCHANGE SERVER-2013

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: (Contact the Counselors for the next available batch)

Fees: ₹ 2,500/- + 15% Service Tax

MICROSOFT PRIVATE CLOUD

Microsoft Certified Solutions Expert [MCSE] Private Cloud

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees: 2,500/- + 15% Service Tax

ADVANCED LINUX

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: (Contact the Counselors for the next available batch)

Fees: ₹ 2,500/- + 15% Service Tax

CCNA SECURITY (Pre requisite is CCNA R&S)

CISCO CERTIFIED NETWORK ASSOCIATE - SECURITY

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹ 7,500/- + 15% Service Tax

CCNP SECURITY (Pre requisite is CCNA Security at ZOOM)

CISCO CERTIFIED NETWORK PROFESSIONAL - SECURITY

Duration: 2 Weeks | 4 Hrs Per Day (starts on 30th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹ 9,500/- + 15% Service Tax

CCIE SECURITY (Pre requisite is CCNA & CCNP Security at ZOOM)

CISCO CERTIFIED INTERNETWORK - SECURITY

Duration: 1 Month | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees:₹15,500/- + 15% Service Tax

VMware vSphere (Pre requisite is MCSE)

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 and Evening: 7.30

Fees: ₹ 4,950/- + 15% Service Tax

VMware vCloud (Pre requisite is VMware vSphere)

Duration: 1 Week | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 9.30 to 11.30

Fees: ₹ 2,500/- + 15% Service Tax

CHECKPOINT FIREWALL

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees: ₹ 5,500/- + 15% Service Tax

We also offer the following courses (Contact the Counselors for the next available batch)

- **CCNA Voice** @ ₹7,500/-
- **CCNP Voice** @ ₹9,500/-
- **CCIE Collaboration** @ ₹15,500/-
- **CCNA Data Center** @ ₹7,500/-
- **CCNP Data Center** @ ₹9,500/-
- **CCIE Data Center** @ ₹15,500/-
- **IPv6 Migration** @ ₹5,500/-

FACULTY

- All Senior Engineers of Zoom working on Live projects
- Training Engineers of British Army, CISCO, CMC, GE, BSNL, Tata Teleservices and Several Corporates etc for 18 Years.

FREE Training

Zoom Technologies offers a number of free resources for the professional development of network engineers.

Register on our website to get access to the video recordings of live sessions on:

- **MCSE – Windows Server 2012**
- **Cisco – CCNA**
- **Cisco – CCNP** **All Tracks (R & S, Security and Voice)**
- **Cisco – CCIE**
- **Exchange Server 2013**
- **Linux** **All Flavors**
- **Advanced Linux**
- **Ethical Hacking and Countermeasure Expert (www.us-council.com)**

Find us at: www.zoomgroup.com

Like us on Facebook and get access to free online webinars as well as special offers and discounts. **https://www.facebook.com/ZoomTechnolgies**

Online Training

Online Training at Zoom is a cost effective method of learning new networking skills from the convenience of your home or workplace.

Taking an online training course has many advantages for everyone (Freshers / Working Professionals). Zoom offers online training for the highly coveted CCNA, CCNP and CCIE courses as well as MCSE, Linux, VMware, Ethical Hacking and Firewalls, IPv6 with more courses planned for the near future. These are live instructor led courses, using Cisco WebEX. Check out our online course offerings at: **http://zoomgroup.com/online_course**

Job Opportunities

There is a high demand for network and security professionals at all times. Apart from job opportunities in India and the Middle East, network and security administrators are also sought-after in the US and Europe.

If you do not have the right skills, then get them now! Choose the experts in network and security training, an organization which has already trained over one hundred thousand engineers.

For the latest job openings in networking and security, register and upload your resume on: **http://zoomgroup.com/careers** or visit zoom to choose job offering from several multinational companies.

ABOUT US

ZOOM Technologies India Pvt. Ltd. is a pioneering leader in network and security training, having trained over a hundred thousand engineers over the last two decades.

We offer a world class learning environment, with state-of-the-art labs which are fully equipped with high-end routers, firewalls, servers and switches. All our courses are hands-on so you'll get much needed practical experience.

The difference between us and the competition can be summed up in one simple sentence. Our instructors are real-time network professionals who also teach.

Zoom has designed, developed and provided network and security solutions as well as training to all the big names in the Indian industry, for the public sector as well as corporate leaders. Some of our clients are:

- TATA
- BSNL
- VSNL
- Indian Railways
- National Police Academy
- Air Force Academy
- IPCL- Reliance Corporation
- CMC
- British Army

No other training institute can boast of a customer base like this. This is the reason for the resounding success of our networking courses. If you do not have the right skills, then get them now. Come, join the experts!

Training Centers in Hyderabad, India.

Banjara Hills

HDFC Bank Building, 2nd Floor,
Road # 12, Banjara Hills,
Hyderabad - 500 034
Telangana,
India.

Phone: +91 40 23394150
Email: banjara@zoomgroup.com

Ameerpet

203, 2nd Floor,
HUDA Maitrivanam, Ameerpet,
Hyderabad - 500 016
Telangana,
India.

Phone: +91 40 23745252
Email: ameerpet@zoomgroup.com

Secunderabad

Navketan Building,
5 Floor, # 501
Secunderabad - 500 003
Telangana,
India.

Phone: +91 40 27802461
Email: mktg@zoomgroup.com

Dilsukhnagar

Ist Floor, # 16-11-477/B/1&B/2,
Shlivahana Nagar, Dilsukhnagar,
Hyderabad - 500 060
Telangana,
India.

Phone: +91-40-24140011
Email: dsnr@zoomgroup.com

website: www.zoomgroup.com